الرهانات القانونية لشبكة الأنترنت و أثرها على السيادة الرقمية للدول

The legal stakes of the Internet and its impact on the digital sovereignty of countries

إكرام بلباي

جامعة عبد الحميد بن باديس بمستغانم

مخبر حقوق الإنسان والحريات العامة

ikram.belbey@univ-mosta.dz

تاريخ الاستلام: 2023/02/01 ؛ تاريخ القبول : 2024/09/17 ؛ تاريخ النشر :سبتمبر2024

ملخص:

تهدف هذه الورقة البحثية إلى معرفة مدى تأثير الأنترنت على سيادة الدول، خاصة بعد الثورة المعلوماتية التي شهدها العالم، والتي نتج عنها تخطي الأنترنت لحدود الدول؛ فالحاجة إلى نصوص تشريعية جديدة تستوعب هذه المستجدات أصبحت ماسة، خصوصا مع دخول تكنولوجيا الإعلام والاتصال ساحة العمل؛ وبروز فكرة السيادة الرقمية للدول على إقليمها.

وخلصت الدراسة إلى أن الدول أضحت تفقد سيطرتها على فضائها السيادي؛ مما دفعها إلى سن قوانين لتحمي بها سيادتها الرقمية وخصوصية مواطنيها، لا سيما مع انتشار ما يسمى بالجرائم ذات التقنية العالية والتي تجاوزت حدود الدول. وبالتالي، لم يعد مفهوم سيادة الدول كما استقر عليه قبل المستحدثات التكنولوجية الجديدة لا سيما الأنترنت، الأداة التي تخطت جميع التوقعات المرصودة لها.

الكلمات المفتاحية: سيادة رقمية؛ أنترنت؛ رهانات؛ جرائم الأنترنت؛ الثورة المعلوماتية.

Abstract:

This research paper aims to know the impact of the Internet on the sovereignty of countries, especially after the information revolution that the world witnessed, which resulted in the Internet crossing the borders of countries. The need for new legislative texts that accommodate these developments has become urgent, especially with the entry of information and communication technology into the workplace. The emergence of the idea of digital sovereignty of states over their territory.

The study concluded that countries are losing control over their sovereign space. Which prompted it to enact laws to protect its digital sovereignty and the privacy of its citizens, especially with the spread of so-called high-tech crimes that crossed state borders. Consequently, the concept of state sovereignty is no longer as it was established before the new technological innovations, especially the Internet, a tool that has exceeded all expectations assigned to it.

Keywords: digital sovereignty; internet; bets; internet crimes; the information revolution.

المؤلف المرسل: إكرام بلباي

مقدمة:

شهد العالم في بدايات القرن العشرين، ثورة تكنولوجية رقمية هائلة، نتج عنها التدفق السريع للمعلومات وتطور تقنيات الأنترنت، هذه الأخيرة جعلت العالم قرية صغيرة مترابطة من خلال شبكة عالمية، متجاوزة بذلك الحدود التقليدية للدول، هذا ما أدى إلى ظهور فكرة "السيادة الرقمية"، وهي فكرة تختلف نوعا ما عن السيادة بمفهومها الكلاسيكي.

فكما هو معلوم، بأن الدول تعتبر أحد الفواعل الرئيسية في المجتمع الدولي، تحافظ على سيادتها الإقليمية بسنها لقوانين وتشريعات لمواجهة أي تعدي عليها؛ من هنا، بذلت جهود قانونية للدفاع عن السيادة الرقمية في شكل قوانين وتشريعات، وكذا أجهزة خاصة لحماية الفضاء الإلكتروني ورصد أي انتهاك للسيادة.

تكمن أهمية الموضوع في معرفة مدى تأثير تكنولوجيا الإعلام والاتصال على السيادة في ظل هيمنة القوى الرقمية ممثلة في الدول الكبرى، وكذا ما نتج عن الأنترنت من سلبيات متمثلة في الجرائم المعلوماتية وانتهاك للخصوصية الرقمية، بالإضافة إلى معرفة الجهود القانونية المبذولة في سبيل الدفاع عن السيادة الرقمية.

أما بالنسبة لأهداف البحث، فهي تتمثل أساسا في معرفة مدلول السيادة الرقمية، ومدى تأثير الأنترنت على مبدأ السيادة، وتداعياتها في ظل العولمة وظهور مسمى تكنولوجيا الإعلام والاتصال؛ كما تكمن أيضا في التعرف على جريمة الأنترنت، التي أضحت من الجرائم الحديثة، والتي تسعى الدول إلى تنظيمها ومحاولة ردعها في ظل انتشارها المهيب وتعدد أوجهها وأشكالها، وذلك في إطار جهودها للدفاع عن سيادتها الرقمية.

ومما سبق، نطرح الإشكال التالي: ما مدى تأثير شبكة الأنترنت على السيادة الرقمية للدول، باعتبارها طرحت أكثر من تحدي في هذا المجال، خصوصا مع ظهور ما يسمى بجرائم الأنترنت، التي تعد من الجرائم الحديثة التي استعصى على بعض الأنظمة القانونية مواجهتها وقمعها؟ وما هي الجهود القانونية للدفاع عن هذه السيادة؟

سنجيب عن هذا الإشكال وفق منهجين، وصفي من خلال التعرف على السيادة الرقمية للدول والتنظيم القانوني للأنترنت. ومنهج تحليلي، من خلال تبيان مدى تأثير شبكة الأنترنت وتداعياتها على السيادة الرقمية للدول والجهود القانونية للدفاع عن هذه الأخيرة. بالإضافة إلى المنهج التاريخي عند دراسة الجذور الأولى للتنظيم القانوني للأنترنت.

وعليه، تم تقسيم البحث إلى مبحثين أساسيين، تناولنا في المبحث الأول بالتفصيل التنظيم القانوني للأنترنت ومبدأ سيادة الدول، وجاء المبحث الثاني يضم أشكال تأثير الأنترنت على السيادة الرقمية والجهود القانونية للدفاع عنها.

1. التنظيم القانوني للأنترنت ومبدأ سيادة الدول

سنتناول في هذه النقطة التنظيم القانوني لكل من مبدأ السيادة والسيادة الرقمية، وكذا التنظيم القانوني لشبكة الأنترنت.

1.1 التنظيم القانوني لمبدأ سيادة الدول

لقد تغير مفهوم السيادة وأصبح أكثر مرونة في ظل التحول الرهيب للنظام العالمي وموازين القوى واقترانها بتكنولوجيا الإعلام والاتصال، فالسيادة بمفهومها العادي ظهر مقابله ما يعرف بالسيادة الرقمية، وهو مفهوم جديد يتناسب في تسميته مع تطور التقني وظهور العالم الافتراضي[1]. ولا تزال العلاقة بين السيادة والسيادة الرقمية بعيدة عن التسوية، ومع ذلك، فهذه مسألة يجب معالجتها للتأكد مما إذا كانت المفاهيم متكاملة ومتكافئة، أو مختلفة ومستقلة كخطوة أولى ضرورية نحو فهم أفضل لفكرة السيادة الرقمية[2]. ولغرض تحديد مفهوم هذه الأخيرة، لا بد من التطرق أولا إلى المفهوم التقليدي للسيادة.

1.1.1 مفهوم السيادة

تعتبر السيادة أهم مبدأ في القانون الدولي فهي أساس بناء هذا النظام القانوني، وبالإضافة إلى كونه أسمى تعبير عن هوية الدولة. علاوة على ذلك، فإن الدولة والسيادة مفهومان لا ينفصلان، وقد تم إضفاء الطابع الرسمي عليهما في ميثاق الأمم المتحدة وفي العديد من المعايير الدولية[3]. غير أن المفهوم التقليدي للسيادة تعرض لعدة هزات وتغيرات مع ثورة المعلومات والاتصالات، خاصة بعد اختراع الأقمار الاصطناعية التي فتحت المجال واسعا أمام البث التلفزيوني المباشر والاتصالات الهاتفية، ثم شبكة الأنترنت التي جعلت العالم قرية صغيرة وسهلت من عملية الحصول على المعلومات وتداولها بعيدا عن رقابة الدولة وسلطتها[4].

إن المادة الثانية من ميثاق الأمم المتحدة في فقرتها الأولى تعترف بمبدأ المساواة بين جميع أعضائها بقولها:" تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها"[5]؛ ومن الناحية القانونية، يمكن تعريف السيادة على أنها من خصائص الدولة، والتي تتمثل في ممارسة الصلاحيات دون أي سلطة تعلوها فتكون بذلك سابقة لوجود الدولة نفسها. وتقوم الدولة التي تعرف على أنها

جماعة من الأفراد مقيمة على رقعة جغرافية معينة بصفة دائمة ومستقرة تكون خاضعة لسلطة سياسية عليا ذات سيادة، على أركان هي الإقليم، الشعب، السلطة، تمارس السيادة التي تميزها عن باقي الكيانات التي تتفق معها في نفس الأركان.

ولها مظهرين خارجي وداخلي، أما الخارجي، فهي تمارسه ضمن التمتع الدولي كفرد منه بمجموعة من الحقوق والواجبات مما يجعلها ذات طابع سلبي، لأنها لا تفرض على الدولة القيام بأعمال محددة، باستثناء القيود التي يفرضها القانون الدولي والمعاهدات والاتفاقيات التي أبرمتها بإرادتها الحرة، كالحق في الانضمام إلى المنظمات والهيئات الدولية، أما عن المظهر الداخلي، فيتمثل في كل الصلاحيات التي تمارسها الدولة على مكونات الدولة إقليم، سلطة، شعب، في إطار القانون وخاصة الدستور في مقابل احترام التزاماتها الدولية، إذن السيادة هي الأهلية القانونية التي هي صفة مميزة للدولة عن باقي أشخاص القانون الدولي العام[6]. ويمكن اعتماد تعريف للسيادة في القانون الدولي بالقول أنها: السيادة هي السلطة العليا للدولة، تضمن استقلاليتها وعدم خضوعها لأي جهة أخرى أو هيئات خارجية.

2.1.1 مفهوم السيادة الرقمية

إن الإشكال بين مفهوم "السيادة الرقمية" والأساس الإقليمي للسيادة بمفهومها الكلاسيكي[7]، يختفي عندما ندرك أنه من أجل ممارسة السلطة على إقليم معين، فإنه من الضروري ممارسة السيطرة على الأنشطة المتاحة عبر الإنترنت في ذلك الإقليم، حيث تربط هذه الرؤية بين المكان والفضاء الإلكتروني.

ويمكن تعريف السيادة الرقمية بأنها: التحكم في البيانات والبرمجيات (مثل الذكاء الاصطناعي) والمعايير والبروتوكولات (مثل G5 وأسماء النطاقات) والعمليات (مثل الحوسبة السحابية) والأجهزة (مثل الهواتف المحمولة)، والخدمات (مثل وسائل التواصل الاجتماعي، والتجارة الإلكترونية)، والبنية التحتية (مثل الكابلات والأقمار الصناعية والمدن الذكية)[8].

وتعرف أيضا بأنها سلطة الدولة "الرمزية والقانونية والواقعية"، التي تمارسها على شركات التكنولوجيا ومواقع التواصل فيما يتعلق بمستخدمي هذه الشركات، الذين هم في نفس الوقت مواطنين لدى هذه الدولة، ولا يجب أن تترك الدولة مواطنيها وكل ما يتعلق بحقوقهم الرقمية لأمزجة المنصات الرقمية خصوصا وأن بيانات المواطن ومعلوماته وكل ما يتعلق به هي حجر الزاوية

في عمل هذه الشركات وهي أساس ربحهم ووجودهم الحقيقي الذي بسببه تبقى هذه الشركات قائمة ليومنا هذا[9].

من خلال ما سبق، يمكن تعريف السيادة الرقمية، أنها بسط الدول لسيطرتها وولايتها القضائية على الفضاء الرقمي المتمثل في الأنترنت. أيضا، لم تكن السيادة الرقمية لتوجد لولا وجود الأنترنت وتخطيه لحدود السيادة التقليدية المتجسدة في الفضاء الفيزيائي المادي للدولة ضمن حدودها الإقليمية[10].

وهنا، يظهر لنا جليا بأن المقصود باستخدام مصطلح "السيادة الرقمية" هو تطبيق السيادة التقليدية للدولة على المجال الرقمي، من خلال تشريعاتها حماية لأمنها وأمن مواطنيها.

2.1 التنظيم القانوني لشبكة الأنترنت

يجب أن تشمل الأهداف الأساسية لرجال القانون فهم الإنترنت وقدراتها، ومدى تطبيق الهيئات للمبادئ القانونية القائمة عليها. كما يجب عليهم أن يسعوا إلى الفهم الكامل للحقائق المرتبطة بتطور الإنترنت والمنتجات والخدمات المرتبطة بها. واستنادًا إلى فهم واقعي دقيق للإنترنت وقدراتها المحتملة، يمكن لرجل القانون أن يطبق بشكل فعال الحقوق والالتزامات والحلول القانونية الحالية على الشبكة بطريقة تتفق مع المصلحة العامة ولا تعيق قدرتها على تحقيق أهدافها التجارية[11].

1.2.1 الجذورالأولى للتنظيم القانوني للأنترنت[12]

إن ما يمكن ملاحظته هو أن التنظيم القانوني للإعلام والاتصال على المستوى الدولي تطور ويتطور دائما بين محورين رئيسيين: وهما التطور التقني لوسائل الاتصال والإعلام من جهة، وسيادة الدولة كمبدأ من مبادئ القانون الدولي من جهة أخرى.

وتتميز القواعد القانونية المطبقة في مجال الاتصال الدولي بخاصتين أساسيتين، تساهمان في صعوبة تنظيمه على المستوى الدولي وهما:

- لهما مصادر مختلفة تقوم بوضعها، ويمكن تصنيف هذه المصادر إلى ثلاثة أصناف من الهيئات والمنظمات الدولية العالمية. وتتمثل في منظمة الأمم المتحدة، الاتحاد الدولي للاتصالات ومنظمة الأمم المتحدة للتربية والعلوم والثقافة والمنظمة العالمية للتجارة.

- أنها تنتمي إلى عدة قوانين بحيث أنه لا توجد شريحة معترف بها تحت عنوان "قانون المعلومات"، ففي كثير من الأحيان اقترن "قانون المعلومات" بحقوق الإنسان فقط، وفي أحيان أخرى ارتبط بقانون الاتصالات البعدية، قانون الفضاء، القانون البريدي، وحقوق الملكية الفكرية أو مجموعة من القواعد الخاصة المؤقتة الضابطة تم الوصول إليها في ظروف مؤسسية وتاريخية معينة.

إن القواعد الدولية المنظمة للاتصال الدولي ذات أصل اتفاقي، فالقواعد الأساسية للتعاون الدولي في مجال الاتصال قد تم تحديدها لأول مرة في إطار الاتفاقية الدولية للتلغراف المصادق عليها بباريس في سنة 1865. وتعتبر الاتفاقية الدولية المتعلقة باستعمال البث الإذاعي لفائدة السلم المصادق عليها في إطار عصبة الأمم بجنيف في 23 ديسمبر 1936، بمثابة الانطلاقة الأولى للتشريع الدولي في مجال الإعلام والاتصال الدوليين. ونتيجة للتطور الحاصل في مجال الاتصال الفضائي جاءت اللائحة رقم 1348 المتعلقة باستعمال الفضاء الخارجي لأغراض سلمية، التي صادقت عليها الجمعية العامة للأمم المتحدة في 1958، والتي جعلت الفضاء الخارجي يهم الإنسانية جمعاء وأن الهدف المشترك هو استعماله لأغراض سلمية. وكرست الجمعية العامة هذا المبدأ الجديد في التعامل الدولي في مجال استعمال الفضاء لخدمة الاتصال الدولي، بالمصادقة على لائحة بتاريخ 20 سبتمبر 1961، تتعلق بالتعاون الدولي في مجال استعمال الفضاء الخارجي لأغراض سلمية. وأكدت اللائحة على أنه يجب على الدول الاتصال كلما كان ذلك ممكنا بواسطة الأقمار الصناعية على أساس قاعدة عالمية.

وقد شهد استعمال الفضاء الخارجي تطورا حاسما بظهور الأقمار الصناعية للبث التلفزيوني المباشر، وسيطرت الولايات المتحدة الأمريكية بداية من الثمانينات على نظم البث التلفزيوني المباشر العالمي، وتوسع استعماله من طرف الاتحاد السوفياتي– سابقا - الذي يرى بأن وضع نظاما للأقمار الصناعية ضرورة سياسية واقتصادية وثقافية ردا على التحدي الأمريكي. ثم استعملته دول أوروبا الغربية في مواجهة هيمنة الولايات المتحدة الأمريكية في مجال تدفق المعلومات، وأصبح يشكل وسيلة عالمية لتدفق المعلومات والثقافة تتجاوز الحدود الوطنية للدول ولا تقف حاجز أمامها، ويصب من الدول المتقدمة باتجاه واحد نحو دول العالم الثالث، مما ترتب عنه مسألتين هامتين في القانون الدولي هما: احترام السيادة الوطنية للدول في جانبها السياسي والثقافي؛ ومسؤولية الدولة عن استخدام الأقمار الصناعية للبث التلفزيوني المباشر[13].

هذا وقد جاء التوجه الدولي لتنظيم الاتصال الدولي، خلال العقد الأخير من القرن العشرين مدعما للموقف الأمريكي، ليس فقط اتجاه دول العالم الثالث وإنما حتى اتجاه الدول الأوروبية، ففي إطار مفاوضات الأورغواي التي توجت بإنشاء المنظمة العالمية للتجارة، تم إقحام قطاع الاتصال ضمن قطاع الخدمات وإخضاعه لقواعد التجارة وحرية السوق، وفقا لأحكام الاتفاق العام لتجارة الخدمات، الذي اعتبر بأنه يسد الفراغ القانوني المتمثل في عدم وجود مجموعة قانونية ملزمة خاصة بتجارة خدمات الاتصال.

وإذا كانت وسائل تكنولوجيا الاتصال التقليدية قد عرفت نوعا من محاولة التنظيم القانوني وذلك في إطار التشريعات الدولية، فإن الإشكال المطروح حاليا هو التطور الكبير والسريع للتكنولوجيات الحديثة على رأسها الأنترنت، هذه الأخيرة التي أصبحت تطرح مشاكل جد معقدة تتجاوز آثارها الإطار الوطني، مما يعيق محاولات تنظيمها سواء داخليا أو في إطار القانون الدولي[14].

وثمة عدة آراء ترى أنه من الصعب إخضاع الأنترنت للتنظيم الدولي؛ إذ يتطلب تحقيق ذلك جهودا خارقة للتوصل إلى اتفاقية توقع عليها كل دول العالم تقريبا. فتنظيم الأنترنت بشكل قانوني من منظور السيادة غير عملي؛ لأن مصدر العمليات والمعلومات يقع خارج نطاق حدود الدولة، ومن ثم خارج نطاق السيادة. فالطبيعة غير الجغرافية للأنترنت تجعل من الصعب تطبيق قوانين مؤسسة بشكل جغرافي، بل يثير النزاع بين القوانين الوطنية والسلطات القضائية، فضلا عن صعوبة تعقب المتهمين وتحديدهم في إطار القدرة على الهروب عبر الحدود الطبيعية، وإذ كان بوسع السلطة المحلية ممارسة الاحتكار، فإنه ليس بوسعها فرض سيطرتها الكاملة على الأنترنت، هذا فضلا عن صعوبة عدم مواكبة المعاهدات الدولية للتطور السريع في تقنيات الأنترنت، فالأنترنت تقدم كل يوم مسائل مبتكرة في حاجة إلى التدخل السريع وطبيعة المعاهدات لا تسعفها[15].

2.2.1 الميزات التقنية للأنترنت

بالنسبة للعديد من القضايا القانونية عبر الإنترنت، يعد فهم الجوانب الفنية للإنترنت أمرًا ضروريًا لإجراء تحليل قانوني مناسب. على سبيل المثال، كيف يمكن للفرد أن يقرر ما إذا كان شخص ما يستخدم الإنترنت قد انتهك حق النسخ دون معرفة ما هي النسخ التي تم إنشاؤها، وفي أي أجهزة ومن قام بها؟ ومع ذلك، هناك صعوبة في وضع التشريعات حول ميزات تقنية تفصيلية للأنترنت، إذ أن هذه الأخيرة سريعة التغيير. ونتيجة لذلك، يفضل تجنب وضع تعريف تشريعي للأنترنت[16].

وتعرف الأنترنت فقهيا بأنها "هي تلك الوسيلة أو الأداة التواصلية بين الشبكات المعلوماتية دون اعتبار للحدود الدولية"، كما يطلق عليها عدة تسميات بحسب الخدمات التي تقدمها أو الخصائص التي تلحقها، كما عرفت الأنترنت بأنها "شبكة تتألف من عدد من الحاسبات الآلية التي ترتبط فيما بينها، أما عن طريق الخطوط التليفونية أو الأقمار الصناعية، لتكون شبكة كبيرة تتيح لمستخدميها الدخول في أي وقت متى كان الحاسب الآلي الخاص به مزود بجهاز مودم".

وتتميز الأنترنت بخصائص معينة ناتجة عن وجود تعاريف مختلفة لها، إذ ليست للتقنية قيمة في ذاتها وإنما هي وسيلة لتنظيم العمل بموضوع ما والاستفادة منه ...فإذا أضيفت المعلومات كموضوع للتقنية فإننا بصدد الأنترنت، هذا ما يدفعنا للقول بأن الأنترنت عالم افتراضي لكل شيء، وهي بجانبها المظلم تجسد تهديدا حقيقيا ضد المجتمع والدولة والسيادة، عالم موازي لعالمنا الحقيقي، فهي شبكة تسمح بانضمام شبكات معلوماتية مختلفة عن طريق استخدام بروتوكول (TCP /IP) والبريد الإلكتروني (Email) ومجموعة الأخبار وصفحات (FTP) وبنوك المعلومات، حيث أن (TCP /IP) هما بروتوكولات التي ميزت الأنترنت عن باقي وسائل الاتصال في البداية، وهما عبارة عن "بروتوكول تقني حول الاتصالات مشتق من بروتوكولين مستقلين هما: بروتوكول التحكم في النقل TCP؛ وبروتوكول أنترنت IP ونظرا لاشتراكهما جرى العمل عادة إلى الإشارة إليهما مجتمعين[17].

والأنترنت ليس لها حدود دولية فهي عابرة لتلك الحدود، كما أنها لا تعترف بالحدود القائمة بين الدول، وهي كذلك ليس لها مالك ولا يوجد جهاز رقابي عليها ولا سلطة مركزية تتحكم بها. فكما نستطيع أن ندخل إلى شبكات الغير يستطيع الغير أن يدخل إلى شبكتنا سواء أكان صديقاً أم عدواً[18].

2 أشكال تأثير الأنترنت على السيادة الرقمية والجهود القانونية للدفاع عنها

في الواقع أن الأنترنت أثرت كثيرا على سيادة الدول، وهذا ما حاولنا التطرق إليه من خلال تحديد أشكال تأثير الأنترنت على سيادة الدول، وكذا الجهود القانونية للدفاع عن السيادة الرقمية.

1.2 أشكال تأثير الأنترنت على سيادة الدول

تؤثر الأنترنت على سيادة الدول بطريقة مباشرة أو غير مباشرة، كما أن حالات التعدي باستخدام الأنترنت ينتج عنه ما يسمى بجرائم التقنية العالية، والتي يكون قد لها مساس بالسيادة.

1.1.2 التأثير غير المباشر للأنترنت على سيادة الدول

التأثير غير المباشر يتمثل بأن الأنترنت سوف تزيد الهوة الرقمية بين الدول الغنية الفقيرة في آلية الوصول إلى الأنترنت، وهذا يجعل الدول النامية أكثر تهميشاً، ففي قطاعات الاتصالات الأخرى كالهاتف والتلكس لديها آليات منظمة لها مثل الاتحاد الدولي للاتصالات، حيث يوجد تنظيم وترتيب دولي ويضمن لكل دولة منضمة حقوقها، أما بالنسبة للأنترنت فإن بعض مكونات الأنترنت الرئيسية تدار حالياً خارج النطاق القانوني الدولي عن طريق الأيكان ICANN [19]، وهذا ما يجعل الدول النامية في وضع اقتصادي صعب، وسبب القلق الحالي هو أن إدارة الأنترنت قد جرت خارج التراكيب المؤسسية القانونية للتنظيم الدولي التقليدي التي وضعت بالأصل لحماية السيادة الوطنية، كما أن الولايات المتحدة قد احتكرت الجذر الموزع حيث أن عشرة منها في الولايات المتحدة بينما اثنان منها في القارة الأوربية وموزع الجذر هو الذي يراقب توزيع مختلف المواقع بحسب التقسيم الجغرافي بحيث يعطي لكل دولة رمزا، وهو يوزع إلى جانب أسماء المجالات الجغرافية، أسماء المجالات التنظيمية مثل دوت كوم، دوت أورغ ...الخ.

2.1.2 التأثير المباشر للأنترنت على سيادة الدول

إن للأنترنت تأثير مباشر على الحياة اليومية وانعكس ذلك على سيادة الدولة بشكل مباشر، وقد يكون التأثير تقني فيما يتعلق بكونه يشكل تهديداً خطيرا للعادات والتقاليد وربما لمفهوم السيادة نفسه، فعن طريق الأنترنت تم تشكيل جماعات المعارضة السياسية وعمل المنظمات غير الحكومية بسهولة أكثر من أية تقنية أخرى سابقة وهذا بسبب طبيعة الأنترنت غير المركزية والمفتوحة للجميع، وبالتالي أصبحت إمكانية تدخل الآخرين في الشؤون الداخلية للدولة تزداد بشكل سريع شيئاً فشيئاً، وعلى جميع الأصعدة، مما أدى إلى حدوث خلل في حدود الدولة. ولقد أصبحت الأنترنت في الوقت الحاضر تشكل تهديداً حقيقياً لقدرة الدولة في السيطرة على السياسة والثقافة والاقتصاد ضمن إقليمها.

أما التأثير الإنساني فيتمثل بأن الاتصالات في الوقت الحاضر تتم عن طريق الأقمار الصناعية، وهذا يؤدي إلى عدم قدرة الدولة على مراقبة الاتصالات كما كانت في السابق والتي كانت تتم عن طرق الاتصالات الأرضية كالتلفون والتلكس وغيرها من الاتصالات، ويبدو بأن الأنترنت تولد تهديدين مهمين الأول يتمثل بأن على الدول أن توافق وتتبنى نظم وقوانين عالمية لكي تحقق رغبتها في المشاركة في اقتصاد عالمي جديد عبر الأنترنت وفي الاتصالات العالمية وهذا اغتصاب للسيطرة

والسيادة الوطنية، ولذلك نجد أن معظم الدول قد وافقت مرغمة على التنازل عن درجة معينة من السيادة لقاء الاشتراك بخدمة الأنترنت عن طريق الأيكان للمشاركة العالمية في الاقتصاد والاتصالات. أما الثاني، فيتمثل في فقدان الدول لسيطرتها على المراقبة والسيطرة والإيقاف للاتصالات الفردية كلما ازدادت تقنية الربط العالمية تطورا[20].

3.1.2 جرائم الأنترنت والمساس بالسيادة

إن مفهوم جرائم ما يسمى بالتقنية العالية، بدأ في بداية الأمر في الستينات والسبعينات، أين ظهرت ما يسمى بجرائم الكمبيوتر والتي اقتصرت على التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي بالاستخدام غير المشروع للبيانات المخزنة في أنظمة الكمبيوتر، وفي الثمانينيات ظهر مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وأنشطة نشر وزراعة الفيروسات الإلكترونية التي تقوم بعمليات تدميرية للملفات أو البرامج، وشاع اصطلاح الهاكرز Hackers. وشهدت التسعينات ثورة هائلة في حقل الجرائم الإلكترونية بل امتدت ليظهر تغيرا واضحا في نطاقها ومفهومها، وكان ذلك بفعل ما أحدثته شبكة الأنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكة المعلومات، فظهرت الجرائم التي تمارس ضد مواقع الأنترنت التسويقية الناشئة والتي يؤدي انقطاعها عن الخدمة لساعات خسائر مالية بالملايين، وانتشرت جرائم نشر الفيروسات عبر مواقع الأنترنت حيث يسهل انتقالها إلى ملايين المستخدمين في ذات الوقت. وأصبح الآن بالإمكان اختراق مواقع البيت الأبيض ووزارة الدفاع الأمريكية.

وبالتالي، تعد جرائم الأنترنت من الجرائم الحديثة التي تستخدم فيها شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها، خاصة وأنها قد ترتكب في دولة ما ويتحقق الفعل الإجرامي في دولة أخرى، أي أنها جريمة ليس لها حدود[21]. أدى هذا إلى تهديد الأمن الوطني والدولي على السواء، لذلك حاولت الدول أن تواجه هذه الأنشطة غير المشروعة الفردية والمنظمة، عن طريق التشريعات الوطنية والدولية، وكذلك عن طريق إنشاء أجهزة متخصصة في مكافحة هذه الجرائم على المستوى الوطني أو على المستوى الدولي[22]،

وتتعدد أنواع وأشكال جرائم الأنترنت ومنها: جرائم تتعلق بالتجارة الإلكترونية، جرائم تتعلق برسائل البريد الإلكترونية، جرائم قرصنة البرامج والشبكات، جرائم قرصنة وسرقة المعلومات، جرائم المتاجرة بالعلاقات الإنسانية، جرائم تهديد الأمن العام، جرائم السطو والسرقة الإلكترونية.

ولم نفصل في التشريعات الوطنية والدولية، وكذا آليات مكافحة جرائم الأنترنت في هذا الفرع، كوننا سنتطرق في المبحث الثاني من هذه الدراسة، إلى مختلف الأساليب التي تم اعتمادها من طرف العديد من الدول والهيئات، في سبيل مكافحة هذه الجرائم والدفاع عن السيادة الرقمية.

2.2 الجهود القانونية للدفاع عن السيادة الرقمية

وهي تنقسم بدورها إلى جهود الدول، وجهود عالمية، وإقليمية، وعلمية كالآتي:

1.2.2 جهود الدول للدفاع عن السيادة الرقمية

بذلت الدول جهودا حثيثة للدفاع عن السيادة الرقمية، ومواكبة التطورات والتغيرات الدولية والرقمية؛ سنتطرق في هذه الجزئية للبعض منها، كالجزائر، روسيا، الصين، والولايات المتحدة الأمريكية.

جهود الجزائر للدفاع عن السيادة الرقمية:

واجه التشريع الجزائري الجرائم السيبرانية، بإصدار قوانين عامة وخاصة، وكفل الدستور الجزائري لسنة 2020 [23]، حماية الحقوق الأساسية والحريات الفردية، كما تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردتها مختلف القوانين التي تحظر كل مساس بهذه الحقوق.

ففي قانون العقوبات[24]، تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي، فعدل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10نوفمبر2004، المعدل والمتمم للأمر رقم 66-106 المتضمن قانون العقوبات، تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، ويتضمن هذا القسم ثمانية مواد من المادة 394مكرر إلى المادة 394مكرر7. [25]

وفي قانون الإجراءات الجزائية، تم تمديد الاختصاص المحلي لوكيل الجمهورية في مجال الجرائم الإلكترونية، طبقا للمادة 37فقرة2 من قانون الإجراءات الجزائية (الأمر 15-02 لسنة 2015)[26]، حيث يمتد الاختصاص المحلي إذا تعلق الأمر بجرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد والتهريب، كما نص على التفتيش في المادة 45 فقرة 2 من نفس القانون المعدل، ونص أيضا بموجب المادة 65مكر ر3فقرة 5 أنه في حالة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات فإن وكيل الجمهورية

المختص يقوم بوضع الترتيبات التقنية دون موافقة المعني، من أجل التقاط وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة. ثم جاء أمر رقم 21-11 المؤرخ في 25 أوت سنة 2021، المتمم للأمر 66-156 المتعلق بقانون الإجراءات الجزائية، والذي نص على استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 211 مكرر 22 منه.

كما سعت الجزائر إلى استدراك الفراغ القانوني لضمان أمن الفضاء الإلكتروني، من خلال تعزيز منظومتها التشريعية خاصة منذ 2009، حيث تم صدور القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بتاريخ 05 أوت 2009[27]. حيث احتوى هذا القانون على 19مادة موزعة على 06 فصول مستمدة من الاتفاقيات الدولية (اتفاقية بودابيست،2001)، وجاء هذا القانون مطابقا للتشريعات الوطنية لا سيما تلك المتعلقة بمحاربة الفساد وتبييض الأموال وتمويل الإرهاب، حيث نص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته[28]. أما بالنسبة للتعريف القانوني للجريمة الإلكترونية، فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون 09-04[29]، وحددت المادة الثالثة منه مجال التطبيق بنصها: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

كما تم إنشاء أجهزة أخرى، منها "السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، نهاية أوت 2022. بالإضافة إلى "المحافظة السامية للرقمنة"، بموجب المرسوم الرئاسي رقم 23-314 المتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، وهي بموجب المادة الثانية منه "مؤسسة عمومية ذات طابع خاص تتمتع بالشخصية المعنوية والاستقلال المالي، توضع تحت وصاية رئيس الجمهورية، وتدعى في صلب النص المحافظة السامية"[30]. ونص الفصل الثاني من المرسوم على صلاحيات المحافظة ومهامها، وأورد في المادة الرابعة منه: "تكلف المحافظة السامية بتصميم الاستراتيجية الوطنية للرقمنة، بالتشاور مع القطاعات المعنية والمؤسسات والقطاع

الاقتصادي والمجتمع المدني. وتكلف أيضا بمتابعة الاستراتيجية الوطنية للرقمنة وتنفيذها. وبهذه الصفة تتولى المهام الآتية:

- اقتراح كل تدبير من شأنه تعزيز السيادة الرقمية وتطوير المنتوج الوطني.

- ... التعاون مع المؤسسات والمنظمات الدولية المماثلة في مجال الرقمنة، طبقا للتشريع والتنظيم المعمول بهما"[31].

وبهذا يكون المشرع الجزائري قد حاول الإلمام بالجوانب التقنية للأنترنت، وبذل جهودا في تجريم ومكافحة أشكال التعدي على السيادة الرقمية، من خلال تعديل القوانين والتشريعات، وإنشاء الأجهزة الخاصة بالحماية.

جهود روسيا للدفاع عن السيادة الرقمية:

من أجل حماية الإنترنت الروسي من "التأثيرات السلبية الخارجية"، تستخدم روسيا أسلوبا خاصا لتجسيد السيادة الرقمية وتوطين البيانات. وتمثل ذلك في القانون الاتحادي FEDERAINYY ZAKON [FZ]، رقم 242 FZ، المؤرخ 21 جويلية 2014 بشأن تعديل بعض تشريعات فدرالية روسيا، ويتعلق الأمر بتحديث إجراءات معالجة البيانات الشخصية في شبكات المعلومات والاتصالات، والذي دخل حيز التنفيذ في عام 2015. هذا الأخير، يتطلب من مشغلي البيانات التأكد من أن يتم تسجيل، وتنظيم وتراكم وتخزين وتحديث/تعديل واسترجاع البيانات الشخصية للمواطنين، باستخدام قواعد البيانات الموجودة في فدرالية روسيا.

وبهذا تكون روسيا قد تبنت السيادة الرقمية كسياسة رسمية، حيث سعت إلى إنشاء شبكة إنترنت روسية قابلة للفصل تماما، والتي أطلق عليها اسم "رونيت" RUNET. ويعكس هذا تحولاً كاملاً في السياسة منذ سنوات، حيث بدأت الحكومة الروسية في فرض سيطرة أكبر على الإنترنت، معترفة بقدرتها الواضحة على المساس بسيادة الدول. وفي عام 2019، وقع الرئيس الروسي فلاديمير بوتين على مشروع قانون "الإنترنت السيادي" ليصبح قانونًا، مما اكتسب صلاحيات واسعة لمراقبة حركة المرور على الإنترنت الروسية والتحكم فيها من خلال ضوابط الأجهزة والبرامج المثبتة في البنية التحتية للاتصالات السلكية واللاسلكية الروسية. وفي عام 2020، فرضت الهيئات التنظيمية الروسية غرامات على شركات فيسبوك وجوجل وتويتر لرفضها تخزين بياناتهم في روسيا[32].

جهود الصين للدفاع عن السيادة الرقمية:

يعود تأكيد الصين لسيادتها على مجالها السيبراني إلى تسعينيات القرن العشرين، عندما تم وضع الإنترنت بشكل صريح تحت سيطرة الدولة. ومنذ ذلك الحين، قامت بتطوير جهاز خاص للإشراف على الفضاء السيبراني الخاص بها، من خلال تصفية المحتوى والرقابة واسعة النطاق التي يطلق عليها اسم "جدار الحماية العظيم"، وبذلك أنشأت في الواقع نظامًا منفصلاً للإنترنت. حيث ترى الصين أن السيادة الرقمية هي الحق المطلق للدولة في السيطرة على بيئة الإنترنت المحلية، والمحتوى الذي يتعرض له المواطنون. وعلى الرغم من سيطرتها على الفضاء السيبراني المحلي، اتخذت الصين خطوات لضمان حماية المعلومات الشخصية، مثل قانون الأمن السيبراني (الذي دخل حيز التنفيذ اعتبارا من جوان 2017)، والذي يحظر على مقدمي الخدمات عبر الإنترنت جمع وبيع المعلومات الشخصية للمستخدمين دون موافقة المستخدم[33]. حيث ينص هذا القانون في المادتين 37 و66 منه، على ضرورة توطين البيانات، أما شروط تسجيل الإسم الحقيقي فقد وردت أحكامها في نص المادة 24 منه. وبخصوص القيود المفروضة على التشفير، فقد نصت المادة 18 من قانون مكافحة الإرهاب على: يتطلب من شركات الاتصالات ومقدمي خدمات الإنترنت توفير خدمات فك التشفير لمساعدة الأمن العام وأمن الدولة على التحقيق في الأنشطة الإرهابية المشتبه بها[34].

جهود الولايات المتحدة الأمريكية للدفاع عن السيادة الرقمية:

ليس للولايات المتحدة الأمريكية موقف واضح بشأن السيادة الرقمية، ويرجع ذلك على الأرجح إلى موقعها المميز في الاقتصاد الرقمي، حيث تتواجد كبرى شركات التكنولوجيا في الولايات المتحدة، ويعتمد عليها العديد من المستخدمين والجهات الفاعلة الأخرى.

ومع ذلك، يدرك البيت الأبيض أن هناك تهديدات أخرى يمكن أن تقوض موقعه المتميز الحالي. والتهديد الرئيسي الذي تم تسليط الضوء عليه في استراتيجيتها الوطنية السيبرانية، المنشورة في عام 2018، هو تهديد الأمن السيبراني، حيث ينظر إليه على أنه أمر أساسي لحماية الأمن القومي الأمريكي وتعزيز رخاء شعبها لأنه جزء لا يتجزأ من جميع جوانب الحياة الأمريكية.

لهذا، اتبعت أجندة سيادية في المجالات ذات الصلة. أحد الأمثلة على ذلك هو قانون الولايات المتحدة بشأن الاستخدام القانوني الخارجي للبيانات (قانون السحابة)(CLOUD) لعام 2018، الذي يسمح لسلطات إنفاذ القانون الأمريكية بالمطالبة بالوصول إلى البيانات التي تحتفظ بها الشركات الأمريكية في الخارج. وقد تعرض هذا القانون، والاتفاق الثنائي ذي الصلة بين الولايات

المتحدة والمملكة المتحدة للسماح بالوصول إلى البيانات عبر الحدود من قبل سلطات إنفاذ القانون، لانتقادات من قبل المدافعين عن الخصوصية[35].

ونلاحظ في الواقع هيمنة الولايات المتحدة الأمريكية والصين على مجال الأنترنت، حيث توفر هذه الدول معايير وتسهيلات لمشغليها في الأسواق الرقمية العالمية. أما عن الدول النامية، فهي تعاني من التبعية التكنولوجية، وتبقى عاجزة عن تحقيق السيادة الرقمية المطلقة في ظل الضعف التكنولوجي الذي تعانيه، من عدم قدرتها على حماية الخصوصية الرقمية، رغم الجهود المبذولة من قبل المشرعين في هذا المجال.

2.2.2 المجهودات العالمية للدفاع عن السيادة الرقمية

والتي جسدتها كل من:

مجهودات الأمم المتحدة للدفاع عن السيادة الرقمية

حيث بدأ الاهتمام بمسألة التصدي للنشاطات المخترقة للسيادة الرقمية للدول، - والمتمثلة في الجريمة المعلوماتية التي لا تعترف بالحدود الوطنية، ولا يمكن أن تواجهها الدول بالوسائل القانونية القمعية التقليدية-، على مستوى الأمم المتحدة أثناء المؤتمر الثامن للأمم المتحدة من أجل الوقاية من الجريمة ومعالجة المنحرفين المنعقد بهافانا (كوبا)، من 27 أوت إلى 07 سبتمبر 1990، الذي تبنت فيه الجمعية العامة قرارا يتعلق بالتشريع في مسألة الجريمة المعلوماتية. وتلتها العديد من الأعمال في المسألة بداية من سنة 1994، وانطلاقا من القرار المذكور، نشرت الأمم المتحدة كتيبا توجيهيا حول الوقاية ومراقبة الجريمة المعلوماتية.

وفي سنة 2000، تبنت الجمعية العامة للأمم المتحدة قرارا حول محاربة استغلال تكنولوجيا المعلومات لأغراض إجرامية. وفي سنة 2004، أنشأت الأمم المتحدة مجموعة عمل حول التلوث البريدي والجريمة المعلوماتية وغيرها من المسائل المتعلقة بالأنترنت. وأثناء المؤتمر الحادي عشر للأمم المتحدة حول الوقاية من الجريمة والعدالة الجنائية المنعقد في بانكوك (تايلاند) سنة 2005، تبنت إعلانا حول ضرورة تجنيس وتوحيد تشريعات محاربة الجريمة المعلوماتية.

كما تبنت الأجهزة التابعة للأمم المتحدة العديد من القرارات في هذا الصدد؛ حيث اتخذت لجنة الوقاية من الجريمة والعدالة الجنائية التابعة لمكتب الأمم المتحدة لمحاربة المخدرات والجريمة تدابير فعالة لمحاربة الاستغلال الجنسي للأطفال.

أما المجلس الاقتصادي والاجتماعي للأمم المتحدة: فقد تبنى قرار حول التعاون الدولي في مسألة الوقاية والتحقيقات والمتابعات والعقوبات المتعلقة بالغش والتعسف والتزوير في الهوية لأغراض إجرامية والمخالفات الملحقة بها عام 2004، كما تبنى المجلس قرارا حول التعاون الدولي في مسألة الوقاية والتحقيقات والمتابعات والعقوبات المتعلقة بالغش الاقتصادي والإجرام المرتبطة بالهوية عام 2007. أيضا تبنى المجلس سنة 2004، قرارا حول البيع عن طريق الأنترنت للمخدرات غير الممنوعة التي تعالج بصورة صريحة لظاهرة مرتبطة بالجريمة المعلوماتية.

مجهودات الاتحاد الدولي للاتصالات للدفاع عن السيادة الرقمية:

يؤدي الاتحاد الدولي للاتصالات دورا ضروريا في تعقيد وتنمية الاتصالات ومسائل الأمن المعلوماتي. حيث كان المبادر للقمتين العالميتين حول مجتمع المعلومات المنعقدتين في جنيف سنة 2003، وفي تونس سنة 2005، اللتين ناقشت فيهما الدول وغيرها من الفاعلين في المجتمع الدولي المواجهة الواجب اتباعها للمشاكل الجديدة المرتبطة بتطور المجتمع العالمي للمعلومات وكذا تطوير قواعد وقوانين ملائمة لها. ليطلق الاتحاد الدولي سنة 2007، البرنامج العالمي للأمن المعلوماتي للاتحاد الدولي للاتصالات، الذي تضمن سبعة أهداف، والمرتكزة على خمسة محاور استراتيجية كبرى المتعلقة بتنمية الاستراتيجيات حول وضع تشريع نموذجي في مسألة الجريمة المعلوماتية[36].

مجهودات مجلس أوروبا للدفاع عن السيادة الرقمية:

تعد اتفاقية مجلس أوروبا للجريمة الإلكترونية لعام 2001، أول مبادرة عالمية وأبرز وأنجح ثمرات التعاون الدولي في هذا المجال حتى الآن، حيث أقرت اللجنة الوزارية لمجلس أوروبا في دورتها رقم 109 بتاريخ 08 نوفمبر 2001، الاتفاقية الأوروبية للجريمة الإلكترونية وتم فتح التوقيع للانضمام إلى الاتفاقية في مؤتمر دولي في بودابست/ المجر في 23 نوفمبر 2001، وفي هذا التاريخ وقعت على الاتفاقية 26 دولة من الدول الأعضاء في مجلس أوروبا البالغ عددها 74 دولة، وعملا بالمادة 37 من الاتفاقية التي تنص على انضمام الدول غير الأعضاء إليها، وقعت هذه الاتفاقية في ذات التاريخ وقعت على الاتفاقية في ذات التاريخ أربعة دول غير أعضاء في المجلس وهي: الولايات المتحدة الأمريكية، اليابان، كندا، جنوب إفريقيا. وتصدرت الاتفاقية ديباجة معبرة عن رغبة الدول الأعضاء في مجلس أوروبا والدول الأخرى الموقعة على الاتفاقية عن رغبتهم وحماسهم للتعاون الدولي بشأن مكافحة الجريمة الإلكترونية من خلال إقرار سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجريمة الإلكترونية وتعزيز التعاون الدولي، وتتكون الاتفاقية من أربعة فصول، كما صدر

بروتوكول إضافي لاتفاقية أوروبا للجريمة الإلكترونية في ستراسبورغ بفرنسا في 28 نوفمبر 2003. أما عن الأهداف الأساسية للاتفاقية فتتمثل في:

- تحقيق التوافق والانسجام بين عناصر الجرائم في القوانين الجنائية المحلية الأساسية، والشروط المتطلبة ذات الصلة في مجال الجريمة الإلكترونية.
- تزويد قوانين الإجراءات الجنائية المحلية في دول الاتحاد الأوروبي وغيرها، بصلاحيات ضرورية للتحقيق وتوجيه الاتهام في الجرائم الإلكترونية وغيرها من الجرائم التي ترتكب باستخدام أنظمة الحاسب الآلي والتعامل مع الأدلة ذات العلاقة بالطابع الإلكترونية.
- إعداد نظام فعال وسريع للتعاون الدولي[37].

3.2.2 المجهودات الإقليمية للدفاع عن السيادة الرقمية

وقد تجسدت فيما يلي:

مجهودات الاتحاد الأوروبي للدفاع عن السيادة الرقمية:

أما عن مبادرات الاتحاد الأوروبي في الدفاع عن السيادة الرقمية، فهي تشمل قانون الأمن السيبراني (2019)، الذي أنشأ نظامًا لإصدار شهادات الأمن السيبراني على مستوى الاتحاد الأوروبي. بالإضافة إلى قانون الأسواق الرقمية (DMA) وقانون الخدمات الرقمي (DSA) اللذين دخلا حيز التنفيذ في نوفمبر 2022. وهما يسعيان إلى تحسين المنافسة من خلال منع المنصات (الأمريكية) الكبيرة من إساءة استخدام مراكزها في السوق[38].

مجهودات منظمة التعاون والتنمية الاقتصادية للدفاع عن السيادة الرقمية:

منذ عام 1985، والمنظمة تحاول محاربة الجريمة المعلوماتية عن طريق التقارير والتوجيهات المختلفة، وفي عام 2007 نشرت المنظمة تقريرا حول المعالجة التشريعية للإرهاب المعلوماتي في التشريع الداخلي للدول، تلبية لطلب مجموعة التخطيط الاستراتيجي التابعة للمكتب التنفيذي للأمين العام للأمم المتحدة المتعلق بإعداد عرض مقارن للحلول التشريعية الداخلية حول مسألة استعمال الأنترنت لأغراض إرهابية.

مجهودات منظمة التعاون الاقتصادي لآسيا والمحيط الهادي للدفاع عن السيادة الرقمية:

حيث أصدر وزراء مجموعة العمل الخاصة بالاتصالات والإعلام التابعة لمنظمة التعاون الاقتصادي لآسيا والمحيط الهادي سنة 2008، إعلانا في بانكوك (تايلاند)، مبينين فيه أهمية متابعة وبلورة تعاون بغرض محاربة الجريمة المعلوماتية.

مجهودات منظمة الكومنويلث (رابطة الشعوب البريطانية) للدفاع عن السيادة الرقمية:

قرر وزراء العدل بمنظمة الكومنويلث إنشاء مجموعة خبراء ترتكز في عملها على معاهدة مجلس أوروبا حول الجريمة المعلوماتية، من أجل إعداد إطار قانوني لمحاربتها لتقدم في مارس 2002، تقريرا وتوصيات في هذا الشأن. وفي نفس السنة، قدمت المجموعة مشروع قانون نموذج حول الجريمة المعلوماتية المرتبطة باستعمال الحاسوب الذي جاء متطابقا مع القواعد المحددة من طرف المعاهدة حول الجريمة المعلوماتية لأنها تحتوي على تعليمات دقيقة وترتكز على الاعتراف بالمعاهدة من قبل مجموعة الخبراء بصفتها قاعدة دولية[39].

مجهودات جامعة الدول العربية للدفاع عن السيادة الرقمية:

صدر قرار عن مجلس وزراء العدل العرب بجامعة الدول العربية بشأن مشروع قانون عربي استرشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها، يتكون من 27 مادة، وضع من خلالها القواعد الأساسية التي يتعين على التشريعات العربية الاستعانة به عند وضع قانون لمكافحة الجرائم الإلكترونية، كما تسعى جامعة الدول العربية إلى إنشاء منظمة عربية تهتم بالتنسيق في مجال مكافحة الجرائم الإلكترونية والتشجيع على قيام اتحادات عربية تهتم بالتصدي لتلك الجرائم، وتفعيل دور المنظمات والإدارات والحكومات العربية في مواجهتها عن طريق نظام الأمن الوقائي[40].

مجهودات منظمة الدول الأمريكية للدفاع عن السيادة الرقمية:

منذ سنة 1999 تعمل منظمة الدول الأمريكية بنشاط من أجل حل مسألة الجريمة المعلوماتية في المنطقة، حيث قامت بالعديد من الاجتماعات في إطار عهدة وزراء العدل أو النواب العامين للدول الأمريكية ليطالبوا في نفس السنة بإنشاء مجموعة خبراء حكوميين حول الجريمة المعلوماتية.

4.2.2 الجهود العلمية للدفاع عن السيادة الرقمية للدول

وجاءت على شكل مقترحات فردية ومؤسسية:

حيث اقترح الفقيه ريتشارد فالك، أن الحل هو التفاهم على وضع "عقد اجتماعي عالمي جديد" لحماية السيادة الرقمية. أما الفقيه لويس كافاري، فقد اقترح وضع تشريع دولي جديد لتنظيم الفضاء المعلوماتي بصفته إرثا مشتركا للإنسانية حتى تتمكن الدول من الدفاع عن سيادتها الرقمية.

كما اقترح البعض وضع مجموعة من الفرضيات في ذلك:

الفرضية الأولى: في حالة وجود موزع أو مقدم خدمة الدخول للأنترنت فوق الإقليم الوطني للدولة التي تعتبر نفسها ضحية، فإن التشريع المحلي هو المطبق على الفعل في كل تحركاته التي ستكون فيها الإمكانيات مضاعفة.

الفرضية الثانية: في حالة وجود الموزع أو مقدم خدمة الدخول للأنترنت خارج الإقليم الوطني للدولة، ستكون المسألة أصعب مثلما هو الحال في أعالي البحار والفضاء الخارجي. فالدولة الضحية بسبب عدم التعاون القانوني الفعال مع دولة الإرسال والنشر لا يمكنها ضبط المسألة. وهو ما يوصلنا إلى مفتاح التنظيم القانوني الممكن.

واقترح البعض الآخر، التحكم في إدارة الأنترنت للدفاع عن السيادة الرقمية، غير أنه حقيقة لا يمكن للدولة محاصرة جميع موردي خدمة الأنترنت ومعرفة مرتكبي الجرائم المعلوماتية وانتشارها. وعليه، لا بد من اتخاذ إجراءات من شأنها محاربة الجريمة المعلوماتية كالآتي:

- تنمية وتطوير ثقافة معلوماتية وليس فقط ثقافة أمنية. إذ لا يكفي تحسيس الشعب بمخاطر الأنترنت والاحتياطات المبدئية التي يجب اتخاذها، بل يجب على المواطنين فهم أيضا أسس وتنظيم النظام الذي يستعملونه.
- دعم مقدرة المنشآت القاعدية للمعلوماتية والاتصالات بالقيام بتدابير أمن تقنية وإجراءاتية وإداراتية منسجمة ووضع نظام قانوني وشرطي فعال بعين المكان.
- القيام بتعاون دولي المعتبر ضروريا في هذا الصدد[41].

خاتمة:

تبقى مسألة السيادة الرقمية للدول حقيقة لا يمكن التغاضي عنها، فبانتشار الأنترنت واختراقه لحدود الدول، صار لزاما وضع ضوابط قانونية للتجاوزات وحالات التعدي التي يمكن أن تطالها. ولا يتحقق ذلك إلا بتظافر الجهود على المستويات الوطنية والعالمية والإقليمية. وعليه، من خلال ما سبق، يمكن استخلاص مجموعة من النتائج واتباعها بالتوصيات اللازمة:

النتائج:

اتخذت السيادة مفهوما آخر غير المفهوم التقليدي، وهو السيادة الرقمية، مما يحتم على الدول البحث عن وسائل قانونية جديدة للتصدي لمن ينتهكها.

أيضا، يمكن القول أن موضوع الأنترنت قد زاد من تعقيد حماية سيادة الدول، خصوصا في ظل هيمنة القوى الرقمية مثل الصين والولايات المتحدة الأمريكية على شبكة الأنترنت.

إن استعمال الأنترنت للتعدي على سيادة الدولة يحدث بصورة متكررة، من قبل أشخاص يجيدون تقنياتها للحصول على المعلومات، مما يعتبر مساسا بالحق في خصوصية الفرد، وتهديدا لسيادة الدول وأمنها، ويحدث هذا التعدي بعدة أشكال وأساليب.

أحدث التطور التكنولوجي والتقني، تغييرا جذريا على المعارف القانونية السابقة. فظهور الأنترنت وتطورها طرح أكثر من رهان وتحدي أدى إلى ضرورة خلق إطار قانوني أكثر تأقلما مع التطورات الحاصلة، خصوصا في مجال انتشار جرائم الأنترنت التي تجاوزت حدود الدول وهي جرائم مستحدثة، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

التوصيات:

على الدول أن تتخذ مختلف الإجراءات الوقائية كالأمن المعلوماتي، وذلك نظرا للتطور الكبير والسريع لتكنولوجيا الإعلام والاتصال، لأن الحلول التشريعية قد تبدو قاصرة إلى حد كبير في ظل هيمنة بعض الدول الكبرى على التكنولوجيا.

ضرورة وضع مشروع معاهدة دولية كخطوة أولية، تهدف إلى صياغة إطار قانوني، يرمي إلى محاربة جرائم الأنترنت على المستوى العالمي.

تقليص الفجوة بين الشمال والجنوب في إمكانية الحصول على الأنترنت، وتعزيز التعاون الدولي في مجال مكافحة جرائم الأنترنت، وتقنينها.

الاهتمام بموضوع السيادة الرقمية وتعزيز الدراسات والبحوث في هذا المجال.

---

[1] مولاي ملياني دلال، الأنترنت والسيادة، مجلة الدراسات الحقوقية، المجلد 7، العدد 1، الجزائر، 2020. ص 387.

[2] Robles-Carrillo, Sovereignty vs Digital Sovereignty, Journal of Digital Technologies and Law, 1(3), (2023). P 675.

[3] Robles-Carrillo, op.cit, p 675.

[4] سحاري محمد، السيادة الوطنية في ظل ثورة المعلومات، مجلة المعيار، العدد 4، الجزائر، 2013. ص ص 40-41.

[5] منظمة الأمم المتحدة، ميثاق الأمم المتحدة، موقع الأمم المتحدة، على الرابط:

https://www.un.org/ar/about-us/un-charter/full-text ، تاريخ الولوج: 20 جانفي 2023، على الساعة: 20:30.

[6] مولاي ملياني دلال، مرجع سابق، ص ص 388-389.

[7] ويطرح فقهاء القانون الدولي، بعض الفروقات بين السيادة والسيادة الرقمية كالتالي: أولا، هناك فرق جوهري بين السيادة والسيادة الرقمية لأن الأولى تنطبق فقط على الدول، بينما تستخدم الأخيرة أيضًا في الإشارة إلى الاتحاد الأوروبي مثلا. ثانيا، بقدر ما يتم تطبيقها على الدول، فإن ذات السيادة ليست نفسها على منظمة دولية، فالسيادة الرقمية ليست بالضرورة نتيجة أو امتداداً للسيادة بالمعنى التقليدي. ثالثًا، في حين أن السيادة الرقمية في حالة الدول لها ما يبررها باعتبارها ضمانة للسيادة التقليدية، فإنها في حالة منظمة دولية مثل الاتحاد الأوروبي، يجب أن تكون وظيفتها مختلفة، لأن الاتحاد الأوروبي يفتقر إلى السيادة. وهناك تفسيرات مختلفة للسيادة الرقمية الأوروبية، ولكن لا يرتبط أي منها بالسيادة التقليدية. أنظر:

Robles-Carrillo, op.cit, p 684.

[8] Anupam chander, Haochen sun, data sovereignty-from the digital silk road to the return of the state, oxford university press, united states of america, 2023. pp 4-5.

[9] السماوي مهند حبيب، سيادة الدول الرقمية، موقع إيلاف، على الرابط:

https://elaph.com/Web/opinion/2021/06/1331270.htm ، تاريخ الولوج : 15 سبتمبر 2022، على الساعة: 14:00.

[10] سعادي محمد، السيادة الرقمية: أو تحديات الأنترنت لمبدأ سيادة الدول في القانون الدولي العام، مجلة الفقه والقانون، العدد 5، الجزائر، 2013. ص 64.

[11] George delta, jeffrey matsuura, law of the internet, walters kluwer publisher, 4th édition, 2021, new york. p 26.

[12] بدأت تقنية الأنترنت في الظهور في الولايات المتحدة الأمريكية منذ عام 1962 أبان الحرب الباردة بينها وبين الاتحاد السوفيتي، إذ قامت مجموعة من العلماء المهرة في وكالة الأبحاث والمشروعات المتطورة واختصارها ARPA وقد عرفت فيما بعد باسم وكالة الأبحاث والمشروعات الدفاعية المتطورة واختصارا DARPA والتابعة لوزارة الدفاع الأمريكية وكانت هذه الانطلاقة عبارة عن ردة فعل علمية كخطوة دفاعية في مواجهة الاتحاد السوفيتي عند قيامه بإطلاق القمر الصناعي سبوتنيك في الفضاء عام 1957، وهو قمر متعدد الأغراض، وبعده قامت الولايات المتحدة بإطلاق الصاروخ explorer في 13 جانفي 1958 وقد تبع ذلك التساؤل عن كيفية تمكن سلطات الولايات المتحدة الأمريكية الاتصال فيما بينها في حالة حدوث كوارث طبيعية أو هجوم ذري أو نووي مثلاً. أنظر: جاسم فائز ذنون، تأثير الأنترنت على السيادة، مجلة البحوث القانونية والسياسية، المجلد 16، العدد1، العراق، 2014. ص 335.

[13]وقد ترتب عن ذلك خلاف بين دول العالم الثالث ودول المعسكر الشيوعي من جهة والولايات المتحدة من جهة أخرى، هذه الأخيرة التي تمسكت بحق وحرية كل دولة في البث الإعلامي من خلال التلفزيون المباشر عبر الأقمار الصناعية. وفي خضم هذا الخلاف جاءت لائحة الجمعية العامة بتاريخ 10 ديسمبر 1982، المتضمنة استعمال الدول للأقمار الصناعية لأغراض التلفزيون الدولي المباشر، وأكدت الأمم المتحدة، من خلالها أن النشاطات القائمة في مجال البث التلفزيوني المباشر عبر الأقمار الصناعية يجب أن تتم بالتوافق مع حقوق السيادة للدول بما فيها مبدأ عدم التدخل، ومع احترام حق كل إنسان في البحث واستقبال ونشر المعلومات والأفكار المعلن عنها في النصوص الأساسية للأمم المتحدة.

وفي ظل واقع الاتصال الدولي المتميز بعدم التوازن بين الدول المتقدمة ودول العالم الثالث، طالبت هذه الأخيرة بداية من السبعينات بإقامة نظام النقاشات الواسعة التي دارت على مستوى اليونيسكو، صادقت الجمعية العامة للأمم المتحدة على اللائحة 201/38 المؤرخة في 16 ديسمبر 1980 تعلن بموجبها موافقتها للإقامة نظام دولي جديد للإعلام والاتصال. هذه اللائحة اعتبرت بمثابة ثورة ففي مجال الإعلام والاتصال الدوليين بتأكيدها على مبدأ التدفق المتوازن للإعلام والمعلومات عارضتها الولايات المتحدة الأمريكية بشدة إلى درجة انسحابها من اليونسكو في 1985، واعتبرتها تمس بحرية الإعلام والتعبير المنصوص عليها في المادة 19 من الإعلان العالمي لحقوق الإنسان. وبعد جدل كبير حول مصطلح النظام الجديد للإعلام والاتصال، صادقت الأمم المتحدة في دورة الجمعية العامة رقم 45، في ديسمبر 1990 على لائحة تحت عنوان: "الإعلام في خدمة الإنسانية" حولت بموجبها اللائحة الصادرة في الثمانينات إلى مجرد نداءات، منتقصة من القيمة القانونية لتلك اللوائح. أنظر: عقة نسيمة، السيادة في ظل المجتمع المعلوماتي، ماجستير، كلية العلوم السياسية والإعلام، جامعة الجزائر، الجزائر، 2004. ص ص105-106.

[14]عقة نسيمة، المرجع السابق، ص ص 104-108.

[15]كدواني شيرين محمد، مصداقية الأنترنت العوامل المؤثرة ومعايير التقييم، العربي للنشر والتوزيع، القاهرة، 2017. ص 115.

[16] Graham smith, internet law and regulation, sweet & maxwell publisher, 4th édition, 2007, united kingdom. P 2.

[17] مولاي ملياني، مرجع سابق، ص ص 393-394.

[18]جاسم فائز ذنون، مرجع سابق. ص 335.

[19]إن الأصل أنه لا يوجد من يتحكم في الإنترنت، ولكن من ثمن الاختراع أول مرة، قد يكون له السبق في احتكار هذه الوسيلة، فعلى عكس وسيلة كالهاتف لها آليات منظمة لها كالاتحاد الدولي للاتصالات، لديها آليات منظمة لهذه الوسيلة تكفل للدول حقوقها على قدم المساواة مع الدول الأخرى، وهو ما لا نلاحظه بالنسبة للإنترنت، رغم أنه كوسيلة ليس له جهة تملكه، إلا أن بعض مكونات الإنترنت الرئيسية تدار خارج الإطار القانوني الدولي، حيث احتكرت الولايات المتحدة الأمريكية وأروبا، رموز الجدر هو الذي يراقب توزيع مختلف المواقع بحسب التقسيم الجغرافي أسماء المجالات مثل com. و org. وغيرها، وهي من مهام الأيكان ICAAN، وجميع الدول والمؤسسات والمنظمات تحتاج هذا التنظيم، وقد جرت العادة بأن يمنح المسمى الأعلى من خلال الهيئة الأمريكية، ويوكل منح المسميات الفرعية أو أدنى إلى جهة وطنية في كل دولة وذلك منعا لاختلاط المسميات مع حقوق العلامة التجارية، وبالتالي تسيطر الأيكان على مسمى نطاق الأنترنت من 1998 بتفويض من الإدارة الأمريكية، وهذا بالسيطرة على إدارة بروتوكولات الأنترنت، إدارة أسماء المجالات، وإدارة نظام الأسماء DNS.

ويتم طلب الحصول على خدمة الإنترنت، لعمل البروتوكولات من شركة الأيكان بدون أي ضمانات، وأي اتفاقيات دولية وبالتالي خارج نطاق القانون، والذي لنا أن نتصور تأثيرها الواضح والأكيد على سيادة الدولة في عالمها المادي والافتراضي معا. أنظر: دلال مولاي ملياني، مرجع سابق ص 397.

[20]جاسم فائز ذنون، مرجع سابق، ص ص 337-338.

[21] غربي أحسن، جرائم الأنترنت بين الجانب التقني وأساليب المكافحة، مجلة الحقوق والحريات، العدد 2، الجزائر، 2015. ص ص 24-25.

[22] جاسم فائز ذنون، المرجع السابق، ص 333.

[23] المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتضمن التعديل الدستوري، المصادق عليه في استفتاء أول نوفمبر 2020. (الجريدة الرسمية رقم 82 لسنة 2020).

[24] أمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 يتضمن قانون العقوبات. (الجريدة الرسمية عدد 49 لسنة 1966)، المعدل والمتمم.

[25] تنص المادة 394 مكرر من (القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004) يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50.000 دج إلى 150.000 دج.

[26] الأمر 15-02 المؤرخ في 23 جويلية 2015 المتضمن تعديل قانون الإجراءات الجزائية. (الجريدة الرسمية عدد 40 لسنة 2015).

[27] القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بتاريخ 05 أوت 2009. (الجريدة الرسمية عدد 47 لسنة 2009)

[28] شحيرط أحمد وقريبيز مراد، تحديات الأنترنت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، المجلد 5، العدد 1، 2022، الجزائر. ص ص 309-310.

[29] فاضل عائشة، المسؤولية الجزائية في الجرائم الإلكترونية (الجزائر نموذجا)، مجلة الحقوق والحريات، المجلد، 11، العدد 1، 2023، الجزائر. ص 617.

[30] المادة 2 من المرسوم الرئاسي رقم 23-314 المتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها، جريدة رسمية عدد 59 مؤرخة في 10 سبتمبر 2023.

[31] المادة 4 من المرسوم الرئاسي رقم 23-314 المتضمن إنشاء محافظة سامية للرقمنة وتحديد مهامها وتنظيمها وسيرها.

[32] Anupam chander, Haochen sun, op.cit, pp 14-15.

[33] Sam wood & others, Digital Sovereignty : the overlap and conflict between states, enterprise and citizens, plum consulting, london, 2020. P 9.

[34] Restrictions on encryption: Article 18 of Counter-Terrorism Law:
(requiring telecoms and ISPs provide decryption services to assist public and state security in investigating suspected terrorist activities) (January 2016). See : Sarah mckune, Shazeda ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, International Journal of Communication 12 (2018), p 3844.

[35] Sam wood & others, op.cit, Pp 15-16

[36] سعادي محمد، مرجع سابق، ص ص 75-78.

[37] مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نشر مجلس التعاون لدول الخليج العربية، سلطنة عمان، 2016. ص ص 60-62.

[38] How Robert, Emmie hine, Luciano floridi, digital sovereignty digital expansionism and the prospects for global AI governance, in Quos vadis sovereignty? philosophical studies series, springer imprint, switzirland, 2023. pp 63-64.

[39] سعادي محمد، مرجع سابق، ص ص 80-81.

[40] العجمي عبد الله، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة، ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن، 2014. ص 92.

[41] سعادي محمد، مرجع سابق، ص ص 75-80.

قائمة المصادروالمراجع:

I- المراجع باللغة العربية:

1- الكتب:

- مجمع البحوث والدراسات بأكاديمية السلطان قابوس لعلوم الشرطة، 2016، الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، نشر مجلس التعاون لدول الخليج العربية، سلطنة عمان.

- كدواني شيرين محمد، 2017، مصداقية الأنترنت العوامل المؤثرة ومعايير التقييم، العربي للنشر والتوزيع، القاهرة.

2- الرسائل الجامعية

- العجمي عبد الله، 2014، المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة، ماجستير، كلية الحقوق، جامعة الشرق الأوسط، الأردن.

- عقة نسيمة، 2004، السيادة في ظل المجتمع المعلوماتي، ماجستير، كلية العلوم السياسية والإعلام، جامعة الجزائر، الجزائر.

3- المقالات في مجلة علمية

- بخدة سفيان ووقاص ناصر، 2021، الطبيعة القانونية للجرائم المستحدثة ووسائل ارتكابها: جريمة الأنترنت كنموذج، مجلة البحوث القانونية والسياسية، المجلد 3 - العدد1، الصفحات 117-139، الجزائر.

- جاسم فائز ذنون، 2014، تأثير الأنترنت على مبدأ السيادة، مجلة كلية الحقوق بجامعة النهرين، المجلد 16- العدد 1، الصفحات 331-348، العراق.

- سحاري مصطفى، 2019، السيادة الوطنية في ظل ثورة المعلومات، مجلة المعيار، العدد 4، الصفحات 40-57، الجزائر.

- سعادي محمد، 2013، السيادة الرقمية: أو تحديات الأنترنت لمبدأ سيادة الدول في القانون الدولي العام، مجلة الفقه والقانون، المجلد 7- العدد 1، الصفحات 384-416، الجزائر.

- شحيرط أحمد وقريبيز مراد، 2022، تحديات الأنترنت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، المجلد 5- العدد 1، الصفحات 302-322، الجزائر.

- غربي أحسن، 2015، جرائم الأنترنت بين الجانب التقني وأساليب المكافحة، مجلة الحقوق والحريات، المجلد 3- العدد 2، الصفحات 33-50، الجزائر.

- فاضل عائشة، 2023، المسؤولية الجزائية في الجرائم الإلكترونية (الجزائر نموذجا)، مجلة الحقوق والحريات، المجلد، 11، العدد 1، الصفحات 615-642، الجزائر.

- مولاي ملياني دلال، 2020، الأنترنت والسيادة، مجلة الدراسات الحقوقية، المجلد 7- العدد 1، الصفحات 384-416، الجزائر.

4- المو اقع الإلكترونية

https://elaph.com/Web/opinion/2021/06/1331270.html
https://www.un.org/ar/about-us/un- charter/full-text

II- المراجع باللغة الأجنبية

1- Books :

- Anupam chander, Haochen sun, 2023, data sovereignty-from the digital silk road to the return of the state, oxford University press, United states of america.

- George delta, Jeffrey matsuura, 2021, law of the internet, walters kluwer publisher, 4th édition, New York.

- Graham Smith, 2007, internet law and regulation, sweet & maxwell publisher, 4th édition, United kingdom.

- How Robert, Emmie hine, Luciano floridi, 2023, digital sovereignty digital expansionism and the prospects for global AI governance, in Quos vadis sovereignty ? philosophical studies series, springer imprint, Switzirland.

- Sam wood & others, 2020, Digital Sovereignty: the overlap and conflict between states, enterprise and citizens, plum consulting, London.

2- Articles:

- Robles-Carrillo, (2023), Sovereignty vs Digital Sovereignty, Journal of Digital Technologies and Law, 1(3), pages 673–690.

- Sarah mckune, Shazeda ahmed, The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda, International Journal of Communication 12 (2018), pages 3835-3855.