# سيادة الدولة الرقمية

## بين

## ضرورة التأصيل وتحديات الوصول

## " دراسة مقارنة"

Digital state sovereignty Between The Necessity Of consolidation And The Challenges Of Accessability

"Comparative Study"

دكتور
صابر عبد الغنى عبد الغنى
مدرس القانون العام
كلية الحقوق – جامعة حلوان

JANUARY 1, 2025

قال تعالى:

"وَمَا قَدَرُوا اللَّهَ حَقَّ قَدْرِهِ وَالْأَرْضُ جَمِيعًا قَبْضَتُهُ يَوْمَ الْقِيَامَةِ وَالسَّمَاوَاتُ مَطْوِيَّاتٌ بِيَمِينِهِ سُبْحَانَهُ وَتَعَالَى عَمَّا يُشْرِكُونَ"

صدق الله العظيم

الزمر الآيه (67)

## مقدمة

أدت تغير طبيعة الجماعة الوطنية والدولية إلى تطور العديد من المفاهيم القانونية التقليدية، فلم يعد التعدى على الحدود الأقليمية، هو التحدى الوحيد الذى يشكل تهديداً لسيادة الدول، بل اصبحت الدول تجد نفسها امام تحديات تضع سيادتها على المحك، منها؛ الفقر والأمراض والأوبئة العالمية ، وكذلك التكنولوجيا الرقمية.

فالحياة فى القرن الواحد والعشرون أصبحت ذات علاقة وطيدة بالشبكة العنكبوتية على اختلاف ما تفرزه من تطبيقات وخدمات؛ هذه التطبيقات تجعل المجتمع دائمًا متصل بالشبكات ذات الأبعاد الكونية وأشهرها المتمثلة فى ( GAFA)

(Google, Apple, Facebook, Amazon)، بالأضافة إلى بعض التطبيقات الأخرى التى تسعى إلى جمع البيانات الخاصة بالأفراد .

هذا التدفق المعلوماتى غير المسبوق، أدى إلى تحكم الشركات والشبكات الاجتماعية فى المجتمع من خلال التعرف على إنماط الحياة وتوجيهها إلى أغراض تخدم الدول، التى تعمل هذه الشركات داخل حدودها ووفق قوانينها[1].

ولهذا فإن التفوق المعلوماتى، يعد من المحددات العالمية للقوة الآن، إذ تم الإدراك بأن الإنترنت، الآن هو المكان الذى يجب على جميع الدول أن تراه محدداً لقوتها، ففى الوقت الذى تقوم فيه الدول ببناء جزء متزايد من بنيتها التحتية الاقتصادية والاجتماعية والسياسية على الإنترنت، لذلك كان لابد أن تكون هناك طريقة لحماية تلك البنية التحتية من معلومات وأنظمة، فالكشف عنها يمكن أن يؤدى إلى تعطيل أو تغيير طريقة عملها، مما يهدد الأمن القومى للعديد من الدول.

الأمر الذى يجعل خطر انتهاك خصوصية الفرد داخل المجتمع يستتبعه خطر على سيادة الدول، إذ تعرضت لمثل هذا الانتهاك فى بنيتها التقنية، وليس ببعيد قضية Combridge Analytica ؛ القضية التى كشفت عن العبث فى بيانات المواطنين الأمركيين، وتوجيههم فى الانتخابات الرئاسية الأمر الذى يشكل معه تهديدًا لسيادة الدولة [2].

---

[1] فأشارت الاحصاءات إلى وجود أكثر من نصف سكان العالم على الإنترنت، وترافق هذا التصاعد فى إعداد مستخدمى الإنترنت، مع تصاعد نسبة القلق، فالانتقال السريع إلى استخدام تكنولوجيا المعلومات والاتصالات لم يسمح للدول بمواكبة هذا التحول السريع بالأضافة إلى عدم قدرتها على وضع سياسيات لمواجهة هذا التحول، فقد انتج عام 2017 معدلات غير مسبوقة من البيانات، تتجاوز فى ضخامتها ما تم انتاجه على امتداد كامل البشرية، الأمر الذى كان له أهميته فى فرض تنبه المعنيين في القطاعين العام والخاص، إلى إدارتها بشكل فاعل، مع مراعاة الجوانب التقنية، والاقتصادية، والإدارية، والقانونية، التي تترتب على ذلك. فمع الانتقال إلى الرقمية، تحولت البيانات إلى قيمة لا تقدر بثمن، ومورد لاقتصاد المعرفة .وفي هذا السياق، تنشر الشركات العاملة، في مجال تقنيات المعلومات، بشكل مستمر، عدد المُستخدمين الموجودين لديها، كما لا تتأخر شركات الإحصاء، عن إصدار تقاريرها حول هذا الموضوع، بهدف تأمين المعلومات اللازمة، للشركات وأصحاب المواقع المختلفة، كي يتمكنوا من وضع خطط انتشارهم، والترويج لمنتجاتهم، وتسويق خدماتهم. للمزيد حول هذا الموضوع راجع **د. منى الأشقر جبور** ، **ود محمود جبور:** البيانات الشخصية والقوانين العربية: - الهمّ الأمني وحقوق الأفراد، المركز العربى للبحوث القانونية والقضائية، 2018، ص 11.

[2] **Kévin Deniau:** Cambridge analytique: tout comprendre sur la plus grande crise de l'histoire de Facebook" , available at: https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/15/02/2020

هذه الأخطار سواء كانت استغلال البيانات أو توجيهها لصالح دول معينة، أدخلت العالم فى مواجهة مباشرة مع هذه الشركات، الأمر الذى خلق تياراً دولياً مناهضاً لعمالقة التكنولوجيا، ينادون بحرية الإنترنت، ويرون أن الحفاظ على بيانات الأفراد والمعلومات، التى يتم تداولها على شبكة الإنترنت، من الأهمية بمكان أن تمتد إليها يد الدولة، لحمايتها وعدم تعرضها لخطر الهجمات السيبرانية، والاعتداء على المعلومات القومية، ولذلك كانت فكرة السيادة الرقمية Digital sovereignty لفرض القانون الوطنى على الفضاء السيبرانى، من الموضوعات التى تحتاج إلى تأصيل قانونى، نظرًا لما يشوبها من التحديات، وما تثيره من غموض فى الأطر التشريعية التى تناولتها.

## موضوع البحث:

لقد أحدث تطور الفضاء السيبرانى والتكنولوجي، تغييراً كبيراً في العالم، أدى إلى إعادة تقييم العديد من المفاهيم القانونية التقليدية، فحقق لها تطورًا هائلاً، ومن هذه المفاهيم التى لحقها التغيير، مفهوم السيادة.

فالإنترنت في أيامه الأولى؛ كان مستخدموه يتحكمون بشبكة الإنترنت، وكان يُعتقد أنها محصنة ضد سيادة الدولة، بسبب ترابطها وطبيعتها العابرة للحدود الوطنية، ومع ذلك، فتوسع عدد مستخدمي الإنترنت في جميع أنحاء العالم، ووضوح تطبيقاتها المحتملة في المجالات العسكرية والسياسية، جعلت الدول تدرك بشكل متزايد فائدة امتلاك قدر معين على الأقل من السيادة على الفضاء السيبرانى، وقد حلت المناقشات الدولية حول مدى وإمكانية تطبيق سيادة الدولة على الفضاء السيبرانى، محل وجهات النظر الأكثر مثالية في العصر السابق([1]).

فالتأصيل لفكرة السيادة الرقمية، وقدرة الدول على فرض قانونها وولايتها القضائية على بنيتها التحتية الرقمية، من الموضوعات التى يجب التطرق إليها، نظرًا لما تمثله من الأهمية لدى الدول، التى تسعى إلى الاستقلال الرقمي فى الوقت الراهن.

فالدول تسعى إلى استرداد جزء من السيادة على البيانات، التى يتم تداولها على الشبكة العنكبوتية داخل إقليمها الوطنى، هذا الأمر، يواجه تحديات كبيرة فى الأنظمة التشريعية والقدرات الاقتصادية، وكذلك مبدأ حرية الإنترنت الذي أضحى من المبادئ التى ترسخ لحق الإنسان فى حرية التواصل على الشبكات العالمية([2]).

---

(1) **See Baezner, Marie; Robin, Patrice**: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), ETH Zürich , November 2018, P5

([2]) **See Luciano Floridi**: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Philosophy & Technology (2020)P369–378.

## إشكالية البحث

**يثير البحث العديد من الإشكاليات التى نسردها على النحو التالى:**

1) يثير مفهوم السيادة الرقمية صعوبات فى تحديده، وكذلك تحديد نطاقه وإمكانية تطبيقه.
2) التطور التكنولوجى السريع، يجعل من الصعب مواكبة التغيرات المستمرة فى المجال الرقمى، وإصدار تشريعات لتنظيم هذا التطور لحماية سيادة الدولة فى الفضاء السيبرانى، إضافة إلى عدم تحديد القواعد التى بناء عليها تمارس الدول سيادة على الفضاء الرقمى، وتعمل على حماية البنية التحتية لها.
3) ماهية القواعد التى تفرض على الشركات التكنولوجية التى تطبق عليها الدولة قانونها، وتأثير ذلك على الشركات الناشئة التى تحتاج للوصول إلى موارد بيانات عالمية وخدمات الحوسبة السحابية العالمية.
4) كيفية التوافق بين حرية الإنترنت التى تتبناها الشركات العاملة فى الفضاء السيبرانى وبين تطبيق الدول لقانونها على هذا الفضاء .

## أهمية البحث وأهدفه.

نسعى من وراء هذه الدراسة إلى الوصول لتأصيل لفكرة السيادة الرقمية للدول، من خلال بيان محددات هذا المفهوم؛ من فضاء سيبرانى، وشركات تكنولوجية وافراد، ودور كل عنصر فى توضيح المفهوم.

فألتاصيل لمفهوم السيادة الرقمية Digital Sovereignty يعزز الأمن القومى للدول، ويعمل على التقليل من التقنيات الأجنبية، التى قد تعرض الدول للهجمات السيبرانية، إضافة إلى السيطرة على البنية التحتية الرقمية الضرورية لمنع حدوث اختراقات محتملة.

أن سيادة الدولة الرقمية تُمكن الأفراد من التحكم فى بياناتهم الشخصية وحمايتها من الاستغلال التجارى أو سوء الاستخدام، وهذا ما يعزز الاقتصاد الوطنى للدول من خلال تطوير البنية التحتية الرقمية لهذه الدول.

---

- **Stephane Couture& Sophie Toupin**: What does the notion of "sovereignty" mean when referring to the digital?, new media & society 2019, Vol. 21(10) 2305–2322.
- **Marin Brenac:** La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique**,** Mémoire Maîtrise en droit, Université Laval Québec, Canada Maître en droit (LL.M.)**.**

ومن الأهداف الخاصة للبحث هى تطوير التشريعات الوطنية، وبناء مراكز بيانات محلية وتقنيات اتصالات تدار داخلياً، ووضع الاستراتيجيات الوطنية التى تعمل على التصدى للهجمات السيبرانية، وحماية الأنظمة الحيوية فى الدولة، فالبحث عن تطبيق السيادة الرقمية ليس مجرد خيار لدى الدول؛ بل هو ضرورة فى ظل تصاعد التحديات الرقمية عالميًا، فتطبيقها يضمن للدول والمؤسسات الوطنية والأفراد القدرة على التحكم فى مستقبلهم الرقمى بطريقة تعزز استقلالهم وأمنهم فى ظل الفوضى المتاحة على الشبكة العنكبوتية.

## منهج البحث

اعتمادنا فى الدراسة على المنهج الوصفى الاستقرائى من خلال التطرق إلى التطور الذى لحق مفهوم السيادة، بفعل ظاهرة العولمة، التى أثرت على مضمون هذا المفهوم، ثم الانتقال بعد ذلك لتحديد ماهية السيادة الرقمية، إضافة إلى المنهج المقارن من خلال عرض القوانين المقارنة، التى تأصل لفكرة السيادة الرقمية للدول، وكذلك أحكام المحاكم الأجنبية التى تكرس لهذه الفكرة، مع عرض نماذج لبعض استراتيجيات الدول التى تسعى إلى امتلاك القدرة على التحكم الكامل فى بياناتهم، أو بنيتهم التحتية الرقمية.

## خطة الدراسة.

أثارنا أن تكون الدراسة منقسمة إلى فصلين كل منهم مبحثين على النحو التالى:

الفصل الأول: السيادة الرقمية ومحدداتها.

المبحث الأول :ماهية السيادة الرقمية.

المطلب الأول:تطور فكرة السيادة.

المطلب الثانى: تعريف السيادة الرقمية.

المبحث الثانى: محددات فكرة السيادة الرقمية.

المطلب الأول: السيادة الرقمية سيادة متعددة.

المطلب الثانى: التنظيم القانوني لتعزيز سيادة الدولة الرقمية.

المطلب الثالث: دور القضاءين الدستورى والإدارى فى الترسيخ لفكرة سيادة الدولة الرقمية.

الفصل الثانى: تحديات السيادة الرقمية.

المبحث الأول: التحديات التى تواجه تطبيق السيادة الرقمية.

المطلب الأول: التحديات القانونية والاقتصادية التى تواجه تطبيق سيادة الدولة الرقمية.

المطلب الثانى: تحقيق التوافق بين مبدأ حرية الإنترنت كمبدأ دستورى وتطبيق الدولة لسيادتها الرقمية.

المبحث الثانى : جهود الدول نحو السيادة الرقمية.

المطلب الأول: جهود الدول الاوروبية لتحقيق السيادة الرقمية.

المطلب الثانى: جهود الصين وروسيا فى تطبيق سيادتهما الرقمية.
المطلب الثالث: جهود الدولة المصرية فى تحقيق سيادتها الرقمية.

# الفصل الأول

# السيادة الرقمية ومحدداتها

**تمهيد وتقسيم:**

أثرت الثورة الرقمية تأثيراً عميقاً على مفهوم السيادة التقليدى، فبينما كان ينظر إليها كونها القدرة على التحكم الكامل فى شؤون الدولة الداخلية والخارجية، أصبح هذا المفهوم الآن يواجه تحديات غير مسبوقة بفعل التكنولوجيا الرقمية.

هذه التكنولوجيا التى ساهمت فى ظهور فضاء جديد وهو الفضاء السيبرانى الذى لا تعترف حدوده بالسيادة التقليدية، إضافةً إلى أهمية البيانات والمعلومات التى تُعد فى الوقت الحالى، موردًا استراتيجيًا، ففرض سيادة الدولة على فضائها الرقمى يساهم فى حماية أمنها القومى، من خلال السيطرة على البنية التحتية الرقمية لديها، إضافة إلى تمكن الأفراد المقيمين فى الدولة من التحكم فى بياناتهم الشخصية وحمايتها من الاستغلال التجارى أو سوء الاستخدام.

فتحديد ماهى السيادة الرقمية و وأهميتها وكيفية تحديد مضمونها، هذا ما سنوضحه من خلال التقسيم التالى.

المبحث الأول :ماهية السيادة الرقمية
المبحث الثانى: محددات فكرة السيادة الرقمية

# المبحث الأول

# ماهية السيادة الرقمية

**تمهيد وتقسيم:**

البحث عن التأصيل لفكرة السيادة الرقمية Digital sovereignty للدول ليس خيارًا لدى الدول القومية فى الوقت الحالى أن شاءت قبلته أو تركته، بل هو ضرورة

فى ظل تصاعد التحديات الرقمية عالمياً، فهذه الفكرة تضمن للدول والمؤسسات والأفراد القدرة على التحكم فى مستقبلهم الرقمى، بالطريقة التى تعزز أستقلالهم وأمنهم فى ظل الامكانيات الهائلة التى لدى الدول الكبرى، وكذلك الشركات العاملة فى الفضاء السيبرانى.

ولتوضيح ماهية السيادة الرقمية للدول، نسعى لعرض موجز لفكرة السيادة وتطورها وتأثير العولمة عليها، ثم الانتقال إلى تعريف السيادة الرقمية فى مطلبين على النحو التالى:

المطلب الأول: تطور مفهوم السيادة.

المطلب الثانى: مفهوم السيادة الرقمية.

## المطلب الأول

## تطور مفهوم السيادة

بادئ ذئ بدء؛ تعتبر فكرة السيادة من المحددات الأساسية المكرسة للوجود السياسي والقانونى للدولة، كما أنها تشكل إحدى الخصائص الجوهرية المرتبطة بالدولة الحديثة، كتنظيم سياسي وقانوني، فالسيادة هى الصفة التى تجعل الدولة ذات كيان سياسي واجتماعي، يحق لها احتكار وسائل القمع المشروعة والضرورية للقيام بالأعباء الملقاء على عاتقها([1])، مثل الحفاظ على النظام العام، والاستقرار فى الداخل وحماية سيادة الدولة وحدودها من الاطماع الخارجية، فهى تمثل الحق الحصري في ممارسة السلطة السياسية العليا على الأفراد الذى يقطنون منطقة جغرافية محددة ([2]).

وتُعد فكرة السيادة فكرة معقدة، وذلك لانه يمكن مناقشتها من زاويتين؛ أولهما، يمكن مناقشاتها من زاوية القانون الداخلى، تلك التى يمكن تسميتها السيادة القانونية

([1]) **See Jens Bartelson**: The Concept Of Sovereignty Revisited, The European Journal Of International Law Vol. 17 No.2,P 464.

([2]) **See Ramona Gabriela& Adela MoișI**: The Concept Of Sovereignty, Journal of Public Administration, Finance and Law, Issue24, 2022, P 292.

التى تفترض قدرة الدول على التشريع بشكل سيادى ومستقل على أراضيها( legal sovereignty presupposes the ability of the state to legislate sovereignly and independently on its territory) ، والثانية، من زاوية القانون الدولى؛ والتى من خلاله تسعى الدول إلى الاستقلال الخارجى، فتنظم سلوكها بعلاقاتها بالدول الأخرى دون تدخل، بالإضافة إلى أنها تطورت فكانت فى البداية تقوم باعتبارها فكرة ذات طابع سياسي، ثم تحولت بعد ذلك تدريجياً، بحيث اصبحت فكرة قانونية ([1])، لذلك سنتعرض لتطور فكرة السيادة من الناحية الكلاسيكية وأثر العولمة على هذا المفهوم([2]).

**أولاً: مفهوم السيادة .**

يُعدّ مفهوم السيادة؛ مفهوم حديث نسبياً([3])، إذ أنها كانت تُعرف بأنها "سيطرة سكان أقليم معين، يحكمه قانون عام، ناتج عن الإرادة الجمعية لأفراده"، وتستند هذه

---

([1]) **انظر د. سعاد الشرقاوى**: القانون الدستورى والنظم السياسية، بدون دار نشر، 2007، ص 61.

([2]) **انظرد. ئالان حمه سعيد صالح ،د. عبدالرحمن كريم درويش**: تأثير العولمة على سيادة الدولة، دراسة مقارنة، مجلة القانون والسياسية، 2016، ص 182.

**زديك الطاهر &العربي رزق الله بن مهيدي**: العولمة وتقويض مبدأ السيادة ، مجلة الباحث، عدد 2، 2003، ص34:38.

وهناك بعض الفقهاء يضع اربعة معانى لماهية السيادة

identifies four meanings of the notion of sovereignty: internal sovereignty, which refers to the organization of public authority within a state and the level of effective control exercised by those in power; the sovereignty of interdependence, which aims at organizing the public authority to control cross-border movements (regulating the circulation of information, ideas, goods, population, pollution or capital beyond its borders); international legal sovereignty, which presupposes the mutual recognition of states or other entities; Westphalian sovereignty, which admits the exclusion of external actors from the configurations of internal authority, For more about this concept, **See Krasner D. St. Sovereignty**: Organized Hypocrisy. Princeton: Princeton University Press, 1999.

([3]) ومصطلح السيادة مصطلحاً قانونياً مترجماً عن كلمة فرنسية Sauverainte وهى مشتقة من الكلمة اللاتينية العامة Superanus والذى تعنى الأعلى، لذلك تعرف السيادة فى أحيان كثيرة بإنها السلطة العليا، وجاءت كلمة السيادة فى اللغة العربية من الفعل يسود سدوداً، أى شرف ومجد؛ ويقال فُلان سَيِّد قومه إذا أريد به الحال، وسائد إذا أريد به الاستقبال والجمع سادة.وخلاصة المعنى اللغوى للسيادة أنها تدل على المُقدم على غيره جاهاً، أو مكانة، أو منزلة أو غلبة، وقوة ورياً وأمراً، للمزيد راجع : لسان العرب لابن منظور، ولم يرتبط المعنى اللغوي والاصطلاحي لصفة "السيد" بنشوء الدولة-القومية(nation-state) ، وإنما سبقها بعقود. فمنذ القرن الثالث عشر استخدم تعبير "السيادة" في أوروبا ليشير إلى صفة أو مكانة الفرد المتفوق أو صاحب المكانة العلوية، أو الحاكم، أو السيد (master).وهي كلمة في أصولها الفرنسية (soverain) تتضمن إلى جانب ما ذكر صفة

السيادة إلى الجغرافيا، والإرادة الشعبية، والمعرفة والثروة والموارد المتاحة، وتسعى كل دولة إلى ضمان استقلالها حتى تتمكن من الاعتماد على نفسها([1]).

ولم تكن السيادة معروفة، بمعناها الحديث حتى القرن السادس عشر، والدال على ذلك كونها نشأت كفكرة مطلقة فى المجتمع الأقطاعى، عندما كانت السلطة الملكية تخوض صراعاً ضد رجال الأقطاع فى الداخل وضد الكنسية فى الخارج، وفى ذلك الحين كانت السيادة تتجسد فى سيادة الملك الذى يتجمع فى يده جميع السلطات وبيده السلطة العليا، ويخضع رعاياه إلى حكمه دون قيد أو شرط([2]).

وذهب Jean Boodin الفقيه الفرنسي الذى يُعد أول من نادى بفكرة السيادة وقدم صياغة حديثة، لتلك الفكرة، إذ عبر عنها فى مؤلفه الشهير الكتب الستة للجمهورية بأنها" السلطة العليا التى يخضع لها المواطنون والرعايا، ولا يحد منها القانون فى الداخل، ويملك هؤلاء الملوك السلطة المستقلة فى مواجهة العالم الخارجى "([3]).

فمفهوم السيادة وفقاً لنظرية Boodin هى السلطة العليا للملك، لا يقيدها قيد، ولا شرط وهى دائمة ومطلقة، وعلى هذا الأساس فإن الحاكم لا يكون مسئولاً عن إعماله إلا إمام قوة عليا تكمن فى السلطة الإلهية، ومن خلال هذا التعريف يلاحظ أن Boodin ينظر ويؤسس للحكم المطلق، وظل هذا المفهوم مهيمن على الفكر القانونى حتى انهيار نظرية الخلط بين شخصية الملك والدولة([4]).

وذهب الفيلسوف الانجليزى" Thomas Hobbes" إلى تأييد نظرية السيادة المطلقة للحاكم، بحيث يتمتع بسلطة مطلقة لا تعلوها سلطة أخرى فى الدولة، وإن كان

---

"اللورد "أو المدير. وفي اللاتينية والإيطالية تعني الرئيس أو المكانة العليا (over) وبالرغم من أن المصطلح كان قد ارتبط ارتباطا وثيقا بالتراتبية الاجتماعية والسياسية، إلا أنه لم يأخذ معناه المؤسسي إلا في القرن السابع عشر عقب توقيع اتفاقية "ويستفاليا" 1648، حيث بات يعني "وجود دولة مستقلة ذات سيادة". إلا أن هذا الارتباط بين الدولة-الأمة وبين السيادة لم يخل من تباينات في تأويله لجهة تحديد الجهة (الشخص أو المنصب أو الكيانية) التي تعتبر مَناط السيادة.

(1) **انظر د. حامد سلطان وآخرون**: الوضع التاريخى لمبدأ السيادة، دار النهضة العربية، 1987، ص 689.

(2) **انظر د. عبد الفتاح ساير:** القانون الدستوري – النظرية العامة للمشكلة الدستورية- ماهية القانون الدستوري الوضعي، دار الكتاب العربى، الطبعة الثانية، 2004، ص 46.

(3) **See Jean Boodin**: six books of the commonwealth translated by m. tooley, basil black well, oxford, Dictinnaire la rouse 2010 P 25.

(4) **see Jorge Emilio Núñez**: "About the Impossibility of Absolute State Sovereignty: The Middle Ages". International Journal for the Semiotics of Law., Volume 28, Issue 2, June 2015 p 237.

هذا الموقف من Hobbes فى دعمه للحكم المطلق، كان انعكاساً طبيعياً للحياة السياسية التى عايشها آنذاك([1]).

بينما ذهب Jean Jacques Rousseau إلى القول بسيادة القانون، وبالحريات السياسية للفرد، وما يترتب عن ذلك من شرعية الثورة على حكم الطغيان، وضرورة الفصل بين السلطات لضمان الحقوق والحريات الأساسية. وفى كتابة العقد الاجتماعى، أشار إلى أن السيادة ما هى إلا تعبير عن الإرادة العامة، كما وصفها أنها مطلقة وغير قابلة للتجزئة([2]).

وأكد المفكر البريطانى " John Austin " على أن تحديد نظرية السيادة، يعتمد على الدولة، كونها نظام قانونى توجد فيها سلطة عليا، تتصرف بوصفها المصدر النهائى للقوة([3])، وتحت تأثير الفقه الالمانى فى هذا الوقت تطور المفهوم واستقر على أن السيادة للدولة وليست للملوك، وبالرغم من الانتقادات الموجه لفكرة السيادة، إلا أنها استقرت فى المواثيق الدولية، ونص ميثاق الامم المتحدة فى المادة الثانية منه على أن المنظمة تقوم على المساواة فى السيادة بين الدول الأعضاء.[(4)]

ويمكن تعريف السيادة بسلطة الدولة العليا التى لا يسمو عليها شئ، ولا تخضع لأحد، وإنما تسمو فوق الجميع وتفرض نفسها على المجتمع"، ويقصد بهذا قدرة الدولة على الانفراد داخلياًً بالقرار السياسي فى جميع القضايا، واحتكارها الأدوات والقوة والاجبار، وعدم خضوعها لسلطة عليا سواء كانت من الداخل أو الخارج.

تشمل السيادة بالفعل، وفقاً للجمعية العامة للأمم المتحدة" الحق غير القابل للتصرف في؛ اختيار وتطوير نظامها السياسي والاقتصادي والاجتماعي والثقافي دون أي شكل من أشكال التدخل من جانب أي دولة"([5])،وفى ذلك تشير محكمة العدل الدولية إلى أن السيادة بحكم الضرورة هى" ولاية الدولة فى حدودها الإقليمية، ولاية انفرادية ومطلقة"([6]).

---

(1) **Tom Sorell**: Hobbes on Sovereignty and Its Strains, https://www.researchgate.net/publication/357139416

(2) **جان جاك روسو**: العقد الاجتماعي، ترجمة عادل زعيتر ، د.ن ، ص 51 .

(3) **Stephen D. Krasner**: Problematic Sovereignty: Contested Rules and Political Possibilities, Columbia University Press, 2001, p 23.

(4) نص فى المادة الثانية من ميثاق الأمم المتحدة على أن" تعمل الهيئة وأعضاؤها في سعيها وراء المقاصد المذكورة في المادة الأولى وفقاً للمبادئ الآتية، تقوم الهيئة على مبدأ المساواة في السيادة بين جميع أعضائها".

(5) قرار الجمعية العامة للأمم المتحدة رقم 2131 (الدورة العشرون) في 21ديسمبر 1965.

(6) Case ( Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua v. Colombia), INTERNATIONAL COURT OF JUSTICE, Summary of the Judgment of 21 April 2022

فالسيادة وفقاً لهذا هى مجموعة من الاختصاصات تنفرد بها السلطة السياسية فى الدولة، وتجعل منها سلطة آمرة عليا، ولعل من أهم هذه الاختصاصات، هو قدرة الدولة على فرض إرادتها على غيرها من الهيئات والأفراد بإعمال قانونها الداخلى من جانبها وحدها، وتكون نافذة من تلقاء نفسها، أى دون توقف على قبول المحكومين لها، ولهذا فالسيادة خصائص تميزها([1]).

**ثانياً: خصائص السيادة .**

1) السيادة مطلقة؛ وتعنى هذه الخاصية أن تكون السيادة غير مقيدة، وإضفاء هذه الخاصية عليها، يجب أن يكون وصفاً مطلقاً، أي أنه لا توجد أيه سلطة أو هئية أعلى منها فى الدولة، وتكون بذلك للدولة السلطة على جميع المواطنين على أقليمها.
2) السيادة غير قابلة للتنازل؛ وهذه الخاصية تدل على أن الدولة لا تستطيع التنازل عن سيادتها، وإلا فقدت ذاتيتها، وعلى هذا فالسيادة والدولة هما فى درجة كبيرة من التكامل والتلازم.
3) السيادة دائمة؛ أي أنها تدوم بدوام الدولة، ففكرة دوام واستمرار السيادة تدل على أن السيادة تدور وجوداً وعدماً مع دوام واستمرار الدولة ذاتها، فتغيير الحكومات، لا يؤدى بالضرورة إلى فقدان أو زوال السيادة، وعليه فالحكومات تتغير ولكن السيادة تبقى وتدوم.
4) السيادة غير قابلة للتجزئة، يجب أن تكون السيادة كلاً واحداً لا تتجزأ ، وبذلك لا تخضع لأى رقابة أو رابطة قانونية من أي نوع تربطها بدولة ما تحد من سيادتها وإلا كانت دولة ناقصة السيادة، أي أنها لا يوجد فى الدولة سوي سيادة واحدة غير قابلة للتجزئة.

**ثالثا: أثر العولمة على مفهوم السيادة**

يعتبر مفهوم السيادة، كغيره من المفاهيم القانونية التى خضعت لتغيير عبر الزمن وتطورت بتطور الفكر القانونى([2])، وهذه الثورة المفاهيمية ليست جديدة في تاريخ السيادة، فقد كان لا بد من إعادة تشكيلها عدة مرات، وخاصة فى ظل التطورات الجيوسياسية([3]).

ولعل من أبرز مظاهر التطور، هى التدفقات عبر القومية التى تسيطر على النظام العالمى الراهن، وهى ما تعرف بظاهرة العولمة، هذه الظاهرة التى تعنى فى

---

([1]) **انظر د. ثروت بدوى** ، النظم السياسية، دار النهضة العربية، بدون تاريخ نشر، ص 39.

([2]) **هشام عوض احمد**، سيادة الدولة بين مفهومها التقليدى وظاهرة التدويل، جامعة الشرق الاوسط ، الاردن، يونيو، 2013، ص 28.

([3]) **Pierre-Yves Quiviger**: Une approche philosophique du concept émergent de souveraineté numérique, Nouveaux Cahiers du Conseil constitutionnel n° 57 (dossier : droit constitutionnel à l'épreuve du numérique) - octobre 2017

الأساس الأتجاه المتزايد نحو تدويل السلع والأفكار و روؤس الأموال على مستوى العالم([1]).

فالعولمة تؤثر على سيادة الدولة، بطرق معقدة ومتداخلة، فبينما تحد من قدرة الدول على اتخاذ قرارات مستقلة فى بعض المجالات، فإنها تقدم فرصًا للنمو والتعاون الدولى فى مجالات أخرى([2]).

فقد كان للعولمة الأثر الإيجابى فى الاقتصاد والتكنولوجيا، والاستفادة الانسانية من المعرفة وتبادل السلع والخدمات وتدفق روؤس الاموال، التى هى أساس انتعاش اقتصاديات جميع الدول الفقيرة، إضافة إلى تعزيز التعاون بين الدول لمواجهة التحديات العالمية مثل التغير المناخى، ومكافحة الأوبئة، وكذلك مكافحة الإرهاب، فالاتفاقيات الدولية كتطبيق للأثر الإيجابى للعولمة، تتيح فرصًا للدول الصغيرة لتحظى بحضور أكبر فى القرارت العالمية([3]).

وعزّزت العولمة من انتشار الأفكار الديمقراطية، وزيادة الوعي بحقوق الإنسان، فعلى الرغم من الفجوات التكنولوجية الهائلة بين الدول إلا أنّ العولمة لعبت دوراً هامًا في إضفاء طابع ديمقراطي على وسائل الإعلام، من خلال شبكات التواصل الاجتماعي، التي شجّعت على تعزيز الانفتاح السياسي، والقضاء على الفساد، وسوء استخدام السلطة، وتحسين التمثيل السياسي، الأمر الذي جعل من العولمة فكرة لتدفق الأفكار السياسية بين الدول([4]).

---

([1]) **Abdifatah Ahmed Ali Afyare**: The impact of globalization on state sovereignty, International Journal of Science and Research Archive ( IJSRA) 2024, 12(02), P 1653–1662. Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1434

([2]) **Ramona Gabriela& Adela Moişi**: The Concept Of Sovereignty, Op.cit, P 295.

([3]) **ئالان حمه سعيد صالح ، عبدالرحمن كريم درويش**، تأثير العولمة على سيادة الدولة، دراسة مقارنة، المرجع السابق، ص186.

([4]) ولا يقتصر التأثير الإيجابي للعولمة على الجانب السياسي والاقتصادي المتمثل فى تدفق رؤوس الأموال بين الدول والأفكار الديمقراطية ولكن هناك جانب آخر للعولمة وهو الجانب الاجتماعي والثقافي فقد عملت العولمة على تعزيز فكرة العدالة المجتمعية على نطاقٍ دولي، فضلاً عن مساهمتها في تركيز أنظار العالم على قضايا مهمة في الإطار المجتمعي، أمّا على الصعيد الثقافي؛ فقد كان للعولمة فضل كبير في تنمية شبكات التواصل المعرفية والثقافية، كما أدّت الى تطوير أنماط الحياة، والسلوكيات الاستهلاكية للأفراد، كما أنّ للعولمة الثقافية الأثر الإيجابي في التغطية الإعلامية؛ وذلك في صبّ اهتمام الشعوب نحو مأساة الأفراد في ظل الزيادة السكانية الضخمة. وساهمت العولمة في تحرير وسائط الإعلام عالمياً؛ فأصبحت بذلك أكثر موضوعيةً وبُعداً عن التعصّب والانحياز، وعزّزت روح الانتماء للمجتمع المحيط، وشجّعت على تطوير مستوى الفنون وتبادلها، وساهمت في زيادة وعي الأفراد حول طبيعة السلع المستهلكة وظروف إنتاجها، كذلك فقد جعلت الحوار بين الثقافات حاجةً أساسيةً لتحقيق التضامن الدولي .

بالإضافة إلى ذلك فقد ساهمت العولمة في نشر التكنولوجيا والابتكار، وذلك بتشجيع التواصل المستمر بين البلدان، ممّا يعني تبادل التطوّرات التكنولوجية والمعرفة بشكلٍ أسرع بينها.

بالرغم من هذه الايجابيات للعولمة، إلا أنها لها من السلبيات التي تؤثر على الأفكار القانونية السائدة مثل السيادة، ومن أهم آثار العولمة التي انعكست سلباً على السيادة الوطنية نجد أنها تتمثل فى ما يلى([1]):

أ) التراجع فى قدرة الدول على اتخاذ القرارات بصورة مستقلة، فتفرض العولمة قيودًا على سياسات الدول، من خلال المعاهدات الدولية، والمنظمات العالمية( مثل منظمة التجارة العالمية والشركات متعددة الجنسيات)، فتجد الدول نفسها مضطرة للأمتثال لقواعد تجارية أو اقتصادية خارجية حتى لو تعارضت تلك القواعد مع مصالحها الوطنية([2]).

ب) انتشار وسائل الإعلام والتكنولوجيا، يساهم فى تقويض الهوية الثقافية الوطنية مما يضعف سلطة الدولة، فى حماية تراثها الثقافى، فالثقافات العالمية تفرض نفسها أحيانًا على الثقافات المحلية، الأمر الذى يضعف معه الانتماء للهوية الوطنية([3]).

ت) من الأثار السلبية للعولمة إيضًا، ضعف التحكم فى الاقتصاد الوطنى، فمن خلال تحرير التجارة والاستثمار، يؤدى هذا إلى الاعتماد على الأسواق

---

([1]) **زديك الطاهر &العربي رزق الله بن مهيدي**: العولمة وتقويض مبدأ السيادة ، مرجع سابق ص35.

([2]) وفى هذا فالمشاركة فى السياسية الدولة تتطلب غالباً التنازل من الدول على قدر معين من السيادة لصالح اتخاذ القرار الجماعى ولذلك يقول البعض

" Impact on National Sovereignty: Participation in international political structures often requires nations to cede some degree of sovereignty in favour of collective decision-making. For example, EU member states must comply with EU regulations and directives, limiting their autonomy in certain policy areas. While globalization offers numerous economic, cultural, and political benefits, it also poses challenges to national sovereignty. Nations must navigate these complexities carefully to harness the benefits of globalization while safeguarding their sovereignty and national interests", **See Ananya Gautam& Shalini Saxena**: The Impact of Globalisation on the National Sovereignty: A Comparative Study, International Journal for Multidisciplinary Research, Volume 6, Issue 2, March-April 2024, P4

([3]) انظر: **د.حسن سمير**، الثورة المعلوماتية عواقبها وآفاقها، مجلة الجامعة دمشق، المجلد 18، العدد 1، 2002، ص 234.

**زغو محمد**: أثر العولمة على الهوية الثقافية للأفراد والشعوب، الأكاديمية للدراسات الاجتماعية والإنسانية. 4 - 2010 ص95.

العالمية، مما يجعل اقتصاد الدول عرضة لتقلبات الاقتصاد العالمى، فنجد أن الشركات متعدد الجنسيات التى يفوق اقتصادها اقتصاد دول تؤثر على سياسات الدول الاقتصادية، وتضعف قدرتها على فرض الضرائب أو سن القوانين الوطنية المتعلقة بهذا الأمر.

وأن كانت السيادة تُعد هى القوة والسيطرة الكاملة والنهائية غير القابلة للنقاش، التى تمارسها الدول على أقليم معين، ويرتبط مفهوم السيادة بفكرة الدولة، ومدى قدرتها على فرض سيطرتها على أراضيها، وتشمل أيضا؛ حرية التعبير عن سيادتها من خلال التعامل مع الدول الأخرى، وعدم قدرة أى من الدول على فرض سيطرتها على أقليم دولة أخرى، وإلى أن جاءت فكرة العولمة لتغير مفهوم السيادة بشكل تدريجى، واصبح عامل الاستقلال مكونا أساسيًا لها.

ونتيجة لهذا، ومع بروز دور تكنولوجيا المعلومات وتغلغلها فى كل نواحى الحياه، وجدت الدول نفسها فى مواجهة مع تراجع المفاهيم القانونية التقليدية؛ كالأمن والسلطة والسيادة، مما جعل مسألة واقع السيادة الوطنية على الفضاء السيبرانى مطروحة، ليظهر مصطلح السيادة الرقمية فى مطلع القرن الحادى والعشرين ، وهو الامر الذي نتناول فى المطلب التالي.

## المطلب الثانى

### مفهوم السيادة الرقمية Digital sovereignty .

بادئ ذى بدء، يعتبر تكييف قيم الدستورية المعاصرة مع المجتمع الرقمي، والتى تهدف في جوهرها، إلى وجود إطار مناسب لحماية الحقوق الأساسية فى البيئة الرقمية، مثار مناقشات عديدة، نظراً لتطور العديد من المفاهيم القانونية، نتيجة لان الحدود بين المجال الرقمي وغير الرقمي اصبحت ضبابية بشكل متزايد، ولذلك كان لابد من البحث عن إطار لتأصيل فكرة سيادة الدولة الرقمية، كونها تعبر عن المستوى التكنولوجيا التى وصل إليه العالم اليوم.

إذا أن المجتماعات اليوم، أصبحت تعتمد على التكنولوجيا المقدمة من الشركات وتتحكم فيها بشكل كبير مثل (الشبكات والمنصات، والاتصالات، والمعلومات، والصحة ، والتجارة، والعدالة، والأمن، وما إلى ذلك)، وهو اتجاه يتزايد مع تطوير الخوارزميات، والأشياء المتصلة بالإنترنت، وكذلك الروبوتات والذكاء الاصطناعي. ومع ذلك، فإن هذه التقنيات محكومة برمز الكمبيوتر؛ ففي الفضاء الرقمي يعتمد تنظيم تلك الأنشطة على المعايير الفنية، والقواعد التي يحددها مهندسو الكمبيوتر أكثر من الاعتماد على القواعد القانونية التي تفرضها الدول، هذا على مستوى الدول، أما على المستوى الدولي، فإن مسألة التحكم في موارد الإنترنت هي التي بلورت مخاوف بعض الدول ، التي ترغب في الحد من الهيمنة الأمريكية على إدارة الشبكة، ولا سيما فيما

يتعلق بالمهام الاستراتيجية لـ ICANN (Internet Corporation for Assigned Names and Numbers)([1]).

ولهذا ظهر مصطلح "السيادة الرقمية"Digital sovereignty" الذى تم استخدامه عام 2012 خلال المؤتمر العالمي للاتصالات الدولية World Conference on International Telecommunications (WCIT-12)، ولا سيما من قبل روسيا والصين ، اللّتان تطالبان باستعادة "حقوقهما السيادية" على إدارة الشبكة ووضع معاهدة دولية لتقاسم المسؤوليات بشكل أفضل([2]).

وفى هذا النطاق، تسعى الدول الغربية هى الأخرى بحماية الفضاء السيبراني الخاص بها. وهذا واضح مع تغير الوضع في أعقاب قضية سنودن في عام 2013([3]).

---

([1]) وهي شركة في كاليفورنيا تأسست عام 1998 للإشراف على إدارة أسماء النطاقات ، وهي الجذر الاستراتيجي للإنترنت. هذه المخاوف اصبحت أكثر حدة لأن الهيمنة التاريخية للولايات المتحدة مصحوبة بحالة شبه احتكار تقني واقتصادي للشركات الأمريكية متعددة الجنسيات ، سواء من حيث أنظمة تشغيل الكمبيوتر أو تطوير التطبيقات الرقمية.

([2]) فتقرر روسيا استناداً إلى الافتراض الذي يعتبر الإنترنت بنية تحتية جديدة للاتصالات على الصعيد العالمي وجزءاً كذلك من البنية التحتية للاتصالات على الصعيد الوطني لدى كل دولة عضو، وبالتالي ضمان النظر إلى موارد الترقيم والتسمية والعنونة وتحديد الهوية في الإنترنت كمورد خرج عبر الحدود، فترى أن يجب وضع وتنفيذ سياسات عامة، بما في ذلك سياسات دولية، بشأن أمور إدارة الإنترنت، وضمان أمن الشق الوطني من الإنترنت، علاوة على التنظيم على أراضيها لأنشطة وكالات التشغيل التي توفر النفاذ إلى الإنترنت أو تحمل حركة الإنترنت بالاضافة إلى وضع سياسات تستهدف تلبية الطلبات العامة فيما يتعلق بالنفاذ إلى الإنترنت واستعمالها و اتخاذ التدابير التنظيمية الضرورية لضمان الأمن والثقة في تقديم خدمات الاتصالات الدولية والعمل على تنفيذ وكالات التشغيل لهذه التدابير.

وتأكيدها على سيادتها الرقمية تؤكد انه يجب اتخاذ أي إجراء تراه ضروريا لحماية حقوقها السيادية ومصالحها في ميدان الاتصالات في حالة تعرض خدمات الاتصالات لديها للضرر بسبب ما قد يصدر عن دول أعضاء أخرى من انتهاك للوائح أو تحفظات أو أعمال.

وفى هذا المؤتمر تحتفظ الصين بحقها فى اتخاذ التدابير التي تراها ضرورية لحماية مصالحها الوطنية:وذلك إذا ما أخفق بلد ما في الامتثال لأحكام لوائح الاتصالات الدولية أو إذا أضرت التصريحات والتحفظات التي تبديها بلدان أخرى بما في ذلك تلك الواردة في الوثيقة 66، بسيادتها الوطنية وخدمات الاتصالات لديها. للمزيد حول هذا الموضوع راجع: الوثائق الختامية للمؤتمر العالمى للاتصالات الدولية المنعقد فى دبى فى الفترة من 3- 14 ديسمبر 2012 ص 62.

([3]) فضح سنودن في عام 2013 أساليب المراقبة الإلكترونية السرية التي تستخدمها أجهزة المخابرات الأمريكية، بما في ذلك التنصت غير القانوني عل المفاوضات بين القادة الأجانب.

وكشفت صحيفة The Washington Post فى 4 ديسمبر 2014 نقلا عن مصادر من بينها وثائق حصل عليها "إدوارد سنودن"، أن وكالة الأمن القومي الأميركية قادرة على تعقب ملايين الأشخاص في العالم من خلال تحديد مواقع هواتفهم المحمولة. ويبلغ حجم البيانات المسجلة والمخزنة من جانب وكالة الأمن القومي (27) تيرابايت أي ضعف حجم كامل البيانات المخزنة في مكتبة الكونغرس، أكبر مكتبة في العالم .

فقد أدى الكشف عن القيام بالتجسس على نطاق واسع لخدمة المصالح السياسية والاقتصادية الأمريكية إلى تساؤل عميق، حول نظام إدارة المساحات الرقمية، لا سيما خلال العديد من مؤتمرات أو المنتديات الدولية المكرسة لهذا الموضوع([1]).

هذا وتجد الدول سيادتها نفسها متنازع عليها، وفي منافسة على حد سواء في ممارسة امتيازاتها التقليدية المرتبطة بالسيادة، فيُعرَّف مفهوم السيادة تقليديًا بأنه السلطة العليا التي تمارس على إقليم محدد، فيما يتعلق بالسكان، من قبل دولة مستقلة، وهى حرة في تقرير مصيرها، واصبحت المفاهيم التقليدية محل مناقشات، في ما يسمى بمجتمع ما بعد ويستفاليان الذي يتميز بالاعتماد المتبادل بين الدول، وصعود قوة المنظمات الدولية، والعولمة الاقتصادية، وتطوير التبادلات عبر الوطنية، والآن

---

**بالأضافة** الى ذلك ذكرت مجلة "Spiegel" الألمانية فى 25 أغسطس 2013 استنادا لوثائق لـ"إدوارد سنودن" أن وكالة الأمن القومي الأمريكية استطاعت اختراق مؤتمرات الفيديو وتجسست على المقر الرئيسي لمنظمة الأمم المتحدة في نيويورك، كما تستخدم في (80 ) سفارة حول العالم برنامج للتجسس بدون علم البلد المضيف. كما أشارت إلى أن الوكالة تجسست على بعثات الاتحاد الأوروبي لدى الأمم المتحدة حتى بعد نقل بعثاته إلى مقرات جديدة .وأن الوكالة تستخدم برنامج داخلي للتجسس تطلق عليه ""Special Collection Service" في أكثر من (80) سفارة وقنصلية على مستوى العالم وذلك بدون علم البلد المضيف. وكشفت الوثائق عن وجود مركز للتنصت تابع للوكالة في مدينة فرانكفورت وآخر في مدينة فيينا .

**و**كشفت الوثائق التى حصل عليها "سنودن" عن هوس الوكالة الأمريكية لجمع البيانات والمعلومات عن الأفراد والدول سواء أن كانت دول حليفة أو عدوة . واستخدمت وكالات الاستخبارت الأمريكية برامج لجمع بيانات عن المستخدمين والمؤسسات سواء كانت حكومية أو غير ذلك من جوجل والفيسبوك وغيرها من الشركات . وهو ما يسمح للمحللين من وحدة تكنولوجيا الخاصة بها الحصول على ملفات الصوت والفيديو، والبريد الإلكترونى، والصور، والوثائق وسجلات الاتصال ومراقبتهم على الإنترنت.

شهدت العلاقات بين العديد من دول أوروبا والولايات المتحدة الأمريكية حالة من التوتر بعد ما نشرمن معلومات حول قيام وكالة الأمن القومى الأمريكية بالتجسس على الدول الأوروبية ومقرات الاتحاد الأوروبى ، وهو ما يخل باعتبارات الثقة المتبادلة التى يجب أن توجد ما بين الحلفاء ما ينعكس بظلاله على حجم التعاون ما بين الدول الأوروبية وأمريكا.

وبالرغم من أن الساسة الأوربيين كانوا على علم بإمكانية تجسس المخابرات الأمريكية سياسيا ، إلا أن أجهزة المخابرات الأوروبية تغض الطرف عن ذلك لأنها كانت تستفيد من النشاطات التجسسية الأمريكية، فالمعلومات التي تحصل عليها الولايات المتحدة من خلال عملية التجسس الواسعة ،كانت تستفيد منها سلطات أوروبية من خلال مبدأ تبادل المعلومات خاصة فى مجال مكافحة الإرهاب

(1) L'UIT a organisé la Conférence mondiale sur les télécommunications internationales (CMTI) à Dubaï, aux Émirats arabes unis, du 3 au 14 décembre 2012. Cette conférence historique a examiné le Règlement des télécommunications internationales (RTI) , qui constitue le traité mondial contraignant destiné à faciliter l'interconnexion et l'interopérabilité internationales des services d'information et de communication, ainsi qu'à garantir leur efficacité et leur utilité et disponibilité pour le grand public.

العولمة الناتجة عن التقنيات التكنولوجية التي أثرت إلى حد كبير على الدول، وتتلاعب بحدودها المادية([1]).

ومفهوم السيادة الرقمية يتجاوز العوامل التقليدية، والحدود الجغرافية المحددة للسيادة الوطنية للدول، فلم يعد مبدأ السيادة تلك المصطلح الذى يقتصر على الأبعاد السياسية، بل تعداه اليوم ليشمل بعداً جديداً تظهر فيه التكنولوجيا الرقمية، كمحدد لهذا المفهوم، وبد ذلك واضحاً من خلال الثورة الرقمية، التى عملت على إحداث تحولات عميقة فى الجماعة الوطنية، حيث برزت استخدامات جديدة وعلاقات جديدة بين المواطنين أثرت بشكل كبير على مدلول السيادة كفكرة قانونية.

ولن كان ارتباط المفهوم التقليدى للسيادة بعوامل تقليدية، كالحدود المادية والقوة البشرية، والسيطرة للسلطة الحاكمة، ولكن مع تطور الاتصالات وحدوث تغييرات جزرية فى هذا المفهوم، وبات من الصعب السيطرة على المعلومات، فى ظل الارتباط بالشبكة الدولية للمعلومات، والتى شكلت تحولاً فى المفاهيم التقليدية المتعارف عليها ومنها مفهوم السيادة.

فالثورة الرقمية عكست التسجيل غير المسبوق فى تسريع تداول المعلومات، وتغلب الفضاء الالكترونى على الحدود المادية للدول، لذلك كانت الدول تسعى إلى الحصول على أسماء النطاقات الخاصة بها على شبكة الإنترنت ([2]).

وفى ذلك يقرر بعض الفقه؛ أن التكنولوجيا الرقمية تشكل فضاًء جديدًا لممارسة الحقوق والحريات، وتؤثر على حدود الفضاء العام والفضاء الخاص، مما يتطلب إعادة تنظيم شروط الضمانات ومضمون هذه الحقوق وتلك الحريات([3])، إضافة إلى إعادة تحديد معالم حرية التجمع، وحرية الرأى والتعبير، ويمكن تعميق الحق في الحصول على المعلومات والمشاركة، على سبيل المثال، يجب تكييف حماية حقوق النشر والخصوصية والكرامة بما يتلائم مع التطورات التكنولوجية، وقد تتأثر الحقوق

---

([1]) **محمد حمشي و عادل زقاغ:** عن السياسة ما بعد الدولية :تعايش بين نظامين أم عصر وسيط جديد؟، مجلة سياسات عربية، العدد54، مجلد 10، يناير 2022، ص11.

(2) **See Jean-Luc Warsmann, Philippe Latombe**: Rapport D'information, Déposé, En Application De L'article 145 Du Règlement Par La Mission D'information Sur Le Thème « Bâtir Et Promouvoir Une Souveraineté Numérique Nationale Et Européenne' N° 4299 Assemblée Nationale , Enregistré À La Présidence De l'Assemblée Nationale Le 29 Juin 2021, P 17.

(3) A. Garapon, « Les enjeux de la justice prédictive », JCP, G, 2017, n° 1, p. 47 ; B. Dondero, « Justice prédictive : la fin de l'aléa judiciaire ? », Dalloz, 2017, n° 10, p. 532.

الأخرى، مثل الحق في التعليم أو الحق في سرية التصويت، بالتكنولوجيات الرقمية الجديدة([1]).

كما يتعلق الأمر بالحقوق الاقتصادية والاجتماعية، مثل ظاهرة "Uberization" التي تمت الأشارة إليها من قبل المجلس الدستوري في عدة مناسبات، مثل القضايا المتعلقة بحقوق العمال أو التحولات الجزرية فى القطاعات المختلفة بفضل الرقمنة([2])، خاصة وأن الثورة الرقمية، تفرز حقوق جديدة، مثل حق النسيان الرقمى وحق المرجعة، أو حرية الوصول إلى الإنترنت، أو حق الوصول إلى البيانات المفتوحة، بما في ذلك الأسس والملامح التي يجب تحديدها([3])، فعندما يغامر الفرد بالدخول إلى عالم غير إقليمي، يجب أن تستند حماية الحريات الخاصة به إلى مبادئ قانونية محددة ومؤكدة بوضوح، وتستند على مجموعة واسعة من الأدوات التنظيمية([4]) التى تؤكدها.

ويلعب القاضي دورًا رئيسيًا فى تنفيذها عملياً، جنبًا إلى جنب مع السلطات المستقلة المختصة بشكل خاص، مثل Commission Nationale Informatique et Liberté (CNIL )، بخبرتها الفنية والقانونية، أو في مجالات تخصصها، أو Haute Autorité pour la Diffusion des Œuvres et la (HADOPI) Protection des droits d'auteur sur Internet ، ومن أجل تسليط الضوء على الأبعاد الرقمية الجديدة للحريات الفردية والعامة التي يحميها الدستور، يعتبر الفقه الدستوري من الممكن التكريس لأبعاد جديدة للحقوق والحريات الأساسية، أو حتى حقوق جديدة في حد ذاتها([5]). وتطبيقاً لهذا فإن حرية الولوج إلى الإنترنت، التي أعلنها المجلس الدستوري سنة 2009، يمكن أن تتحول إلى حق قابل للتنفيذ. ويجري تدريجيًا توضيح نطاق وحدود حق الوصول إلى المعلومات على شبكة الإنترنت، في إطار مبدأ الشفافية المنصوص عليه اللائحة العامة لحماية البيانات،

---

([1]) **See Annie I. Anton & Travis D. Breaux:** Digital privacy: theory, policies and technologies, Article in Requirements Engineering · March 2011, P 2.

([2]) Décision n° 2015-484 QPC du 22 septembre 2015.

([3]) **محمد عرفان الخطيب**: ضمانات الحق في العصر الرقمي من تبدل المفهوم .. لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويتي، مجلة كلية القانون الكويتية العالمية، ملحق خاص – العدد3 - الجزء الأول - مايو 2018، ص 254،

**(4)** **E. Geffray**: « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Nouveaux Cahiers du Conseil constitutionnel, n° 52, 2016, p. 7.

**(5)** **I. Falque Pierrotin:** « La constitution et l'Internet », Nouveaux cahiers du Conseil constitutionnel, n° 36, 2012, p. 37.

والأمر الذى جعل الفقه يطالب بإمكانية إدراج حماية البيانات الشخصية في متن الدستور الفرنسى([1])([2]).

لذلك نقول أن الدولة ذات السيادة هي دولة مستقلة "معترف بها داخل حدودها من قبل المجتمع الدولي" وتمارس "سلطة الإدارة والولاية القضائية" على سكانها، ومع نقل هذا المفهوم إلى المجال الرقمي، فإنه من الصعب تحديد كينونته.

فإذا كانت السيادة الرقمية تشير عمومًا إلى حقيقة مؤدها، هى أن تفرض الدولة سلطتها وتمارس صلاحياتها في الفضاء الإلكتروني، فإنها تتصادم أيضًا مع قضايا أكثر واقعية، مثل الاعتماد التكنولوجي أو التحكم في البيانات الشخصية للمستخدمين.

ففي الواقع، تهدف حركة التأصيل لفكرة السيادة الرقمية، التي بدأت قبل عشر سنوات تقريباً، إلى استعادة جزء من السلطة التي تُمارس في الفضاء الرقمي الذي اعتبره المروجون لها في وقت مبكر جدًا بمثابة هروب من نفوذ الدول. ونص إعلان استقلال الفضاء الإلكتروني، الصادر عام 1996، على غياب سلطة الحكومات في هذا النظام الرقمى، فكتب جون بيرى بارلو" "إلى حكومات العالم الصناعي، أنتم العمالقة المُرهَقة من اللحم والفولاذ، أرسل لكم هذه الرسالة من الفضاء الإلكتروني، العالم الجديد للعقل. باسم المستقبل، أطلب منكم تركنا وشأننا. أنتم لستم مُرحبًا بكم بيننا. ليس لديكم أي سيادة حيث نجتمع"([3]).

---

(1) C. const., 2015-713 DC, 23 juillet 2015, Loi relative au renseignement ; E. Derieux, « Vie privée et données personnelles – Droit à la protection et »droit à l'oubli« face à la liberté d'expression », Nouveaux Cahiers du Conseil constitutionnel, n° 48, 2015, p. 21. D. Dechenaud, Le droit à l'oubli numérique : données nominatives, approches comparées, Larcier, 2015.

(2) ويفترض أن يكون هناك موقفًا مستقبليًا للمجلس الدستوري بشأن حق الإذعان، وهو امتداد تقني للحق في النسيان، والذي اعترفت به محكمة العدل التابعة للاتحاد الأوروبي منذ عام 2014. ويلعب هذا دورًا رئيسيًا، استنادًا إلى ميثاق الحقوق الأساسية للاتحاد والاتفاقية الأوروبية لحماية حقوق الإنسان لحماية مصالح المستخدمين الأوروبيين، في سياق متوتر بسبب قضية سنودن. إنها تناضل من أجل ضمان مستوى عالٍ من حماية البيانات الشخصية (إبطال قانون (Safe Harbor 26) )، وتضمن حماية خصوصية مستخدمي الإنترنت الذين يستخدمون خدمات الشركات الأمريكية (إصدارات درع الخصوصية التي اعتمدتها المفوضية الأوروبية ودخلت حيز التنفيذ في 1 أغسطس 2016، بالتنسيق مع CNIL وشبكة CNILs الأوروبية (G29). لأنه فيما يتعلق بإدارة العالم الرقمي وكذلك فيما يتعلق بحماية الحقوق والحريات، فمن الممكن أيضًا، وقبل كل شيء، على المستوى الأوروبي معالجة القضايا بشكل مفيد.

dans un contexte de transfert et de stockage extra-territorialisé des données, les enjeux en termes de souveraineté et d'équivalence des protections du Microsoft Ireland case, cf. United States Court of Appeals for the Second Circuit, 14 juillet 206, Microsoft Corp. v. United States.

(3) Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I

ولذلك سرعان ما وجدت الدول نفسها أمام تحدي على سيادتها، بسبب صعود العولمة الرقمية التي تتجاهل الحدود والقوانين الداخلية، الأمر الذي يسمح لأقوياء الويب بفرض قواعدهم الخاصة، أو حتى الوصول إلى مرتبة "الدول غير المادية".

ونتيجة لهذا ظهر مصطلح السيادة الرقمية، كنتيجة لمواجهة الآثار السلبية التي افرزتها العولمة. وأثرت على فكرة السيادة، حيث أن العولمة وجدت لها أرض خصبة فى ظل تطور الاتصالات وتبادل الأفكار والمعلومات إلى مواطنى الدول، مما تقلص معها دور الحدود المادية للسيادة.

وبما أن مفهوم السيادة تطور مع مرور الوقت، ولم يتم تحديد معناه على الإطلاق، فإنه لا يوجد تعريف قانوني واضح للسيادة الرقمية، ولعل ذلك يرجع إلى حداثة المفهوم وقلة البحوث الأكاديمية التى تناولته.

فمصطلح السيادة الرقمية يعود إلى بداية العقد الأول من القرن الحادى والعشرين، وتحديدًا في عام 2011 قدم **Pierre Bellanger**، رئيس شركة سكيروك، أول محاولة لتعريف السيادة الرقمية للدول، وعرفها على أساس أنها" السيطرة على حاضرنا ومصيرنا كما يتجلى ويسترشد باستخدام التكنولوجيا وشبكات الكمبيوتر"([1]).

ونجد تعريف أخر لها فى الوثائق التي عرضها مشروع X-Gaia والتي نشرتها الوزارة الفيدرالية الألمانية للشؤون الاقتصادية والطاقة، تم تصوير سيادة الدلوة الرقمية على أنها "جانب من جوانب السيادة العامة"([2])، ويتم تعريفه على النحو التالي "إمكانية تقرير المصير المستقل من قبل الدولة والمنظمات فيما يتعلق باستخدام وهيكلة

---

ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.**See John Perry Barlow**: A Declaration of the Independence of Cyberspace, Davos, Switzerland, February 8, 1996

(1) **See Pierre Bellanger:** La Souveraineté Numérique, Les Dîners De L'institut Diderot

(2) Federal Ministry for Economic Affairs and Energy (BMWi), 'Digital Sovereignty in the Context of Platform-Based Ecosystems' (n 2) 6.

الأنظمة الرقمية نفسها، والبيانات المنتجة والمخزنة فيها، والعمليات الموضحة نتيجة لذلك"([1]).

وفقاً لهذا التعريف فالسيادة الخاصة بالبيانات بدورها جزءاً لا يتجزأ من مفهوم سيادة الدولة الرقمية، مما يدل على القدرة الكاملة لدى الدول في السيطرة على البيانات المخزنة والمعالجة وكذلك القرار المستقل بشأن من يسُمح له بالوصول إليها([2]).

وإذا ما تم مقارنة هذه التعريفات مع العناصر الأساسية للسيادة الحديثة، والتي يقصد بها السلطة العليا للدولة على إقليم ما، واستقلالها عن الكيانات الخارجية، فيمكن ملاحظة أن هناك مجموعة من أوجه التشابه والاختلاف، من حيث الأصول العامة للمصطلح، سيادة الدولة الرقمية لا تعمل على تقويض المبادئ الأساسية للسيادة التقليدية، وإنما تحافظ على تأصيلها العام، ومع ذلك، فإن مفهوم السيادة الرقمية يتم استخلاصه فى إطار النظام البيئي الرقمي. وأن كانت السيادة الرقمية لا تتناول فكرة الأقليم باعتباره عنصراً اساسيًا لها، كما هو راسخ فى التعريف التقليدى لمفهوم السيادة، لكنها تشير إلى شكل من أشكال السيطرة على الأصول الرقمية، والتي يمكن أن تكون كيانات مادية وغير مادية، وبالتالي من المحتمل أن تقع في مساحة تتجاوز الحدود المادية.

علاوة على ذلك، فإن السيادة الرقمية ليست من صلاحيات الدولة حسب، بل إنها أيضا من اختصاص "المنظمات" الخاصة المخولة بهذه السلطة. ولا تستطيع الدول وحدها أن تواجه تحديات عالم تحكمه العولمة؛ فالمنظمات الإقليمية والدولية، مثل الاتحادالأوروبي، تنشأ بالضرورة لتكملة وظائف الدول([3]).

فالمنتجات المعلوماتية غير مقتصرة على دولة بعينها، فلم يعد فى مقدور أى دولة أن تكتفى بالمعلومات التى تنتجها سواء من أجهزتها الحكومية أو من خلال مواطنيها، وإنما لازماً عليها الاستعانة بالقطاع الخاص، المتمثل فى شركات الاتصالات وتكنولوجيا المعلومات لإدارة وتنظيم هذا الكم الهائل من البيانات الرقمية المتداولة لدى الدول.

وفقا لهذ أعلنت الحكومة الألمانية فى يوليو 2020، في برنامجها الرسمي لرئاستها للمجلس الأوروبي، عن نيتها "تأسيس السيادة الرقمية كفكرة مهيمنة للسياسة

---

(1) ) Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2) 7.

(2) Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2) 7.

(3) See **Cf. Edoardo Celeste**, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) 33 International Review of Law, Computers & Technology P 76.

الرقمية الأوروبية، وهذه مجرد واحدة من الأحداث العديدة الأخيرة، وإن كانت بارزة جدًا، حيث استخدمت الحكومات مصطلح السيادة الرقمية لنقل فكرة مفادها، أنه يجب على الدول إعادة تأكيد سلطتها على الإنترنت وحماية مواطنيها وشركاتها من التأثيرات المتعددة، وتحديات تقرير المصير في المجال الرقمي([1]) .

ويري جانب من الفقه فى تعريفه للسيادة الرقمية، أن هذه الفكرة تدور حول بسط الدولة لسيطرتها وولايتها القضائية على الفضاء الرقمي، والمتمثل فى الإنترنت، ووفقاً لهذا الرأي لا يتحقق هذه السيادة الرقمية إلا في ظل الدول التي لديها سيطرة فعلية على تكنولوجيا البيانات دون غيرها من الدول.

ولذلك فسيادة الدولة الرقمية تشير إلى قدرة الدولة على التصرف فى الفضاء الإلكترونى، وعلى احترام قواعدها من مختلف الفاعليين فى العالم الافتراضى، وفى هذا الصدد يتيح هذا التعبير عن الصعوبات التى تواجهها الدول التى تقوم بالاضطلاع بوظائفها التقليدية فى مواجهة الجهات الفاعلة عبر الوطنية القوية، التى تتمتع بتقدم تكنولوجى لا جدال فيه، والتى تعتمد عليها فى بعض الاحيان، لأنها تحتاج إلى التكنولوجيا لتتمكن من تحقيق سيادتها، ومن ثم فأن مصطلح السيادة الرقمية له بلا شك جانب قانونى، يشير إلى صلاحيات الدولة وقدرتها على تنظيم عمالقة التكنولوجيا المعاصرة.

وبذلك فيختلف المفهوم التقليدى للسيادة عن كيفية إستخدامه فى مجالات السيادة الرقمية، فالمتعارف عليه أن السيادة التقليدية هى سمة من سمات الدول المعترف بها دوليًا، والتى تمارس السلطة العليا على الأراضى، فى حين أن السيادة الرقمية هى استراتيجية فعالة تهدف إلى بسط سلطة الدولة على البنية التحتية الرقمية فى سياق عالمى([2])

ولكن السؤال الأهم فى هذا الخصوص ما هي الأهمية التي تعود علينا من التأصيل لفكرة سيادة الدولة الرقمية .

تتجلى أهمية التأصيل لفكرة السيادة الرقمية فى عدة نواحي هي:

**1) الأهمية السياسية.**

---

(1) **Christian Katzenbach and Thomas Christian Bächle:** Digital sovereignty, nternet Policy Review, Volume 9 , Issue 4, : 17 December 2020, p 2.

(2) **See Samuele Fratini:** Quels Sont Les Modèles De Mise En Œuvre De La Souveraineté Numérique ? [Entretien] 11 juin 2024, https://www.sciencespo.fr/public/chaire-numerique/2024/06/11/entretien-quels-sont-les-modeles-de-mise-en-oeuvre-de-la-souverainete-numerique-par-samuele-fratini/

السيادة الرقمية وسيلة فعالة في أعادة ثقة المواطنين فى الدولة، فالتأصيل لهذه الفكرة يعمل على حماية مؤسسات الدولة وحماية خصوصية المواطنين، وبياناتهم الشخصية وحماية البنية التحتية للدول([1]).

فقد واجهت الدول والشركات العاملة فى التكنولوجيا الرقيمة، وكذلك المواطنين تهديدات كبري، وما قضية **Cambridge Analytica** إلا خير دليل علي استخدام بيانات الافراد والتأثير على التصويت، و هي فضيحة سياسيّة كُبرى تفجّرت في أوائل عام 2018 عندما تم الكشف عن أنّ شركة **Cambridge Analytica** قد جمعت «بيانات شخصية» حولَ ملايين الأشخاص على موقع فيس بوك من دون موافقتهم قبل أن تستخدمها لأغراض «الدعاية السياسية».

وُصفت الفضيحة من قِبل الكثيرين على أنها «لحظة فاصلة» في الفهم العام للبيانات الشخصية كما أدّت إلى حدوث هبوطٍ كبيرٍ في سعرِ أسهم شركة فيسبوك العالميّة فيما دعا آخرون إلى «تنظيمٍ أكثر صرامة» لاستخدام شركات التكنولوجيا للبيانات الشخصية.

---

[1] ومن الأهمية بمكان الأشارة إلى الوثائق التي نشرتها صحيفة "**The Guardian** " البريطانية يوم الأربعاء 31 تموز/يوليو 2013 و التي تفيد أن الاستخبارات الأمريكية تستخدم منذ 2008 برنامجا سريا لمراقبة الإنترنت **يدعى xkeyscore** يتيح لها أن تعرف "تقريبا كل ما يقوم به مستخدم ما" على الإنترنت ويسمح لوكالة الأمن القومي المراقبة، وبشكل آلى، رسائل البريد الإلكتروني، والدردشة، وتصفح الإنترنت لأي شخص في العالم. فإن تحليل هذا البرنامج بيّن أن وكالة الأمن القومي الأمريكية تستخدم أدوات مجانية مفتوحة المصدر للتجسس.

هذه الوثائق التي نشرتها "**The Guardian** " تكشف كيفية عمل برنامج ،**Xkeyscore** فإن هذا البرنامج يسمح بالوصول إلى تاريخ التصفح والبحث، والبريد الإلكتروني والدردشة الفورية لأي فرد في العالم طالما أن الوكالة لديها عنوان**IP Internet Protocol Adress**.

فهنالك ما لا يقل عن 500 خادم موزعين في جميع أنحاء العالم تشغل برنامج Xkeyscore. هذا يعني أنه بإمكان وكالة الأمن القومي الأمريكية الغوص في العديد من قواعد البيانات و"مشاهدة" محتوى الرسائل المتبادلة على مواقع التواصل الإجتماعي كـ"فيس بوك" وغيره من مواقع التواصل الإجتماعي، كما يمكن للوكالة جمع البيانات من خلال إنشاء مجموعات وفقا للّغة المستخدمة والمناطق الجغرافية التي تعتبرها "مناطق غير آمنة" والتي يتم نشر الرسائل منها وذلك لتمييز لغة التواصل "العادية" من تلك التي يمكن أن تعتبر لغة "غير طبيعية" التي تتناول موضوعات "خطيرة". أي بمعنى أخر فهرسة ،وبشكل نمطي، المواضيع الحساسة وفقا لمعايير الدفاع المحددة من قبل وكالة الامن القومي.

و تطبيق Xkeyscore. موزع على خوادم لينكس **Red Hat** وايضا يستخدم خادم الإنترنت **Apache** و يحفظ البيانات التي يجمعها في قاعدة بيانات **MySQL**.

كما يفيد التحليل لهذه الوثائق أن وكالة الأمن القومي تستخدم أدوات أخرى مفتوحة المصدر كمنصة تحرير النصوص **Vim** لتحرير الشيفرة المصدرية للبرامج . كذلك تستخدم الـ **NSA** برنامج **rsync** المفتوح المصدر لمزامنة الملفات عن بعد.

**وتحدد الأهمية السياسية فى نقطتين هما.**

**أولاً**: مسؤولية الحكومات عن الهجمات الإلكترونية التي تنطلق من أراضيها، كونها تقع تحت سيادة الدولة. فالسيادة تمنح حقوقاً للدول، وتفرض عليها التزامات، وفقاً لما ذكرته محكمة العدل الدولية فى بيانها عن النتائج المترتبة على الأعتراف بسيادة الدول. بالتالي، يُفترض أن تتحكم الدول في بنيتها التحتية الإلكترونية، وتمنع استخدامها عن قصد أو عن غير قصد لإلحاق الضرر بالجهات الحكومية وغير الحكومية خارج حدود الدولة. وبناءً عليه، تخضع الدولة ومواطنيها ممن شاركوا في الهجمات الإلكترونية لنطاق السيادة الرقمية.

**ثانياً**: مسؤولية الحكومات عن فضائها السيبراني، وأمن بنيتها التحتية، وأمن مواطنيها من الهجمات الداخلية والخارجية ومقدرتها على صد الهجمات والاستجابة للأحداث السيبرانية، والاجراء الاستباقي في الحروب السيبرانية، اضافة إلى التعافي بعد الهجمات والعودة للعمل بأقل الخسائر وأسرع وقت.

لذلك لا يقتصر مفهوم السيادة الرقمية على المنظور القانوني الكلاسيكي الصارم المرتبط بسلطة الدول. وإنما يشير بأوسع معانيه إلى قوة القيادة والحق في تقرير المصير في العالم الرقمي.

**2) الأهمية الاقتصادية.**

فى ظل التطور الهائل فى تكنولوجيا المعلومات لا يوجد مجتمع آمن من التجسس العلمى والاقتصادي والتجاري، وعلية يجب على الدول حماية الشركات وسرية البيانات الموجودة لديها، وذلك عن طريق الاهتمام بسيادتها الرقمية التى تعتبر الوسيلة الأمثل لضمان آمن لهذه المعلومات والبيانات، واستردادها فى حالة حدوث هجوم عليها.

فأطلق على البيانات النفط الجديد، فاصبحت فى عصرنا الحالى واحدة من أهم الموارد الاقتصادية فى العالم، كما كان النفط هو أساس الثروة والتنمية فى القرن العشرين، فالبيانات فى العصر الحالى هى التى تقود قاطرة التنمية فى كثير من الدول.

وفي هذا السياق، تنشر الشركات العاملة، في مجال تقنيات المعلومات، بشكل مستمر، عدد المستخدمين الموجودين لديها، كما لا تتأخر شركات الإحصاء، عن إصدار تقاريرها حول هذا الموضوع، بهدف تأمين المعلومات اللازمة، للشركات وأصحاب المواقع المختلفة، كي يتمكنوا من وضع خطط انتشارهم، والترويج لمنتجاتهم، وتسويق خدماتهم([1]).

---

**([1]) See Romina Bandura, Madeleine McLean, and Sarosh Sultan:** Unpacking the Concept of Digital Public Infrastructure and Its Importance for Global Development, December 20, 2023, https://www.csis.org/analysis/unpacking-concept-digital-public-infrastructure-and-its-importance-global-development

فالتكريس لفكرة السيادة الرقمية يحمل أهمية اقتصادية كبيرة، حيث يعني قدرة الدول على التحكم في بياناتها؛ وبنيتها التحتية الرقمية، وسياساتها التكنولوجية دون الاعتماد على جهات أجنبية، في عالم يتحول بشكل متسارع نحو الاقتصاد الرقمي، نتيجة لهذا تصبح السيادة الرقمية عاملًا استراتيجيًا لتحقيق النمو الاقتصادي المستدام والحفاظ على الأمن القومي الاقتصادى للدول.

وتحمل الأهمية الاقتصادية لتكريس لسيادة الدولة الرقمية فى جوانب هى:

1) تعزيز الاقتصاد المحلي.

من خلال تطوير بنية تحتية رقمية وطنية، مما يقلل من الاعتماد على الشركات الأجنبية، ويعزز الإنفاق داخل الدولة، فبناء شركات تكنولوجيا محلية يقود إلى خلق وظائف جديدة وتحفيز الابتكار، إضافة إلى حماية البيانات كمورد اقتصادى، والتكريس لسيادة الدولة الرقمية يضمن أن تبقى هذه البيانات داخل حدود الدولة، ويمكن استخدام هذه البيانات فى تحليل الأسواق المحلية، مما يخلق بيئة لتحسين الخدمات العامة، ودعم الشركات الناشئة، الأمر الذى يقلل من التبعية التكنولوجية، ويعمل على تطوير حلول تكنولوجية محلية تتناسب مع اجتياجات الدول، ويقلل من الاعتماد على شركات أجنبية يمكنها أن تتحكم في الوصول إلى هذه البيانات([1]).

2) تعزيز الأمن اقتصادى.

ضمان حماية الاقتصاد من الهجمات السيبرانية أو سياسات الشركات الكبرى التي قد تؤثر على الاقتصاد المحلي. فالتكريس لهذا المفهوم يمنع الشركات الأجنبية من استخدام البيانات بطرق تضر بمصالح الاقتصاد الوطنى، الأمر الذى يشجع على الابتكار وريادة الأعمال ويدعم الشركات الوطنية الصغيرة والمتوسطة لتطوير منصات وتطبيقات وطنية بديلة لتلك الأجنبية([2]).

بالتالي، التكريس لسيادة الدولة الرقمية ليس مجرد اختيار، بل ضرورة اقتصادية واستراتيجية لدول تسعى لتحقيق الاستقلال الرقمي والنمو المستدام في عصر الاقتصاد الرقمي.

**ثالثًا: الأهمية الاجتماعية.**

تتجلى الأهمية الاجتماعية في عدة جوانب:

1) حماية الخصوصية والأمان الرقمي:

---

**([1]) See Marin Brenac:** La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique, op.cit, p 46.

**([2]) See Jukka Ruohonen:** The Treachery of Images in the Digital Sovereignty Debate, Minds and Machines (2021) 31:439–456.

فالسيادة الرقمية؛ تعني أن الدول لديها القدرة على حماية بيانات مواطنيها من الاختراقات أو الاستغلال من قبل جهات أجنبية أو شركات عالمية، الأمر الذى يعزز ثقة الأفراد في استخدام التكنولوجيا ويمنحهم شعورًا بالأمان.

2) تعزيز الهوية الثقافية:

من خلال التحكم في المحتوى الرقمي، يمكن للدول تعزيز لغتها وثقافتها في الفضاء الرقمي، مما يساهم في الحفاظ على الهوية الوطنية والاجتماعية في عصر العولمة.

3) تعزيز الديمقراطية والمشاركة المجتمعية:

عندما تكون البيانات والبنية التحتية الرقمية تحت سيطرة الدولة، يمكن ضمان شفافية أكبر في العمليات الحكومية، وتعزيز مشاركة المواطنين في صنع القرار عبر منصات رقمية آمنة، فسيادة الدولة الرقمية تساعد في الحد من تأثير الجهات الخارجية التي قد تحاول التلاعب بالرأي العام أو نشر معلومات مضللة عبر الإنترنت، مما يعزز الاستقرار الاجتماعي والسياسي، وكذلك تعمل على تمكين المجتمعات المحلية، من خلال تطوير حلول رقمية محلية، يمكن تلبية احتياجات المجتمع بشكل أفضل، مثل تقديم خدمات تعليمية أو صحية رقمية تلائم الثقافة المحلية([1]).

خلاصة القول أن التأصيل لسيادة الرقمية ليست مجرد قضية تقنية، بل هي قضية قانونية واجتماعية واقتصادية وسياسية، تعكس قدرة المجتمع على التحكم في مصيره الرقمي، وحماية مصالحه في عصر يتسم بالاعتماد المتزايد على التكنولوجيا.

لذلك يمكن تعريف السيادة الرقمية باعتبارها مجالا تقنيًا قانونيًا يتميز بمطالبات الدول والشركات والأفراد بالتحكم فيه ولذا، فإن هذا المصطلح يُستخدم للتعبير عن قوة الدول واستقلالها في الفضاء السيبراني، أي أنها قادرة على الاستقلالية والتحكم والسيطرة على البنى التحتية الرقمية، والتقنيات ووسائل الاتصالات.

## المبحث الثانى

## محددات فكرة السيادة الرقمية

شهدت الجماعة البشرية تطوراً ملحوظاً فى مجال التكنولوجيا الرقمية وتطبيقاتها، الأمر الذى جعل حياة الأنسان أكثر ارتباطاً بالأجهزة الألكترونية والعوالم الافتراضية، إضافة إلى أن التكنولوجيا الرقمية ألقت بجُل تأثيرها على تطور الأنظمة السياسية والمفاهيم القانونية، وعلى الرغم من الإيجابيات التى حملتها الثورة الرقمية

---

**([1]) See Gary Jeffrey**: Constitutional Identity, The Review of Politices 68, 2006. P 367.

لتسهيل حياة الأفراد، إلا أنها حملت معها العديد من المخاطر والتهديدات على كافة المستويات سواء للفرد أو للدول.

الأمر الذى اصبحت معه السيادة القومية للدول فى صراع جديد مع التطورات التكنولوجيا، التى ظهرت من خلالها ساحات سيادية جديدة، دفعت الدول والشركات العالمية ذات الميزانيات الضخمة إلى التناحر لفرض سيطرتها عليها.

ولذلك فمحددات السيادة الرقمية لا يتواقف على مدى قدرة الدولة على فرض سيادتها على بياناتها وبيانات افرادها داخل الفضاء السيبرانى، وأنما هناك محددات تتمثل فى معرفة ماهية الفضاء السيبرانى وقدرة شركات الاتصالات وتكنولوجيا المعلومات بالأضافة إلى مدى استجابة الأفراد، ولذلك تحدد السيادة الرقمية من خلال ثلاث مطالب هما .

المطلب الأول :السيادة الرقمية سيادة متعددة.

المطلب الثانى: التنظيم القانوني لتعزيز سيادة الدولة الرقمية.

المطلب الثالث: دور القضاءين الدستورى والإدارى فى ترسيخ لفكرة السيادة الرقمية.

## المطلب الأول

## السيادة الرقمية سيادة متعددة .

بادئ ذى بدء، تتحدد فكرة السيادة الرقمية، لأى دولة من خلال العديد من الأمور، التى من خلالها تستطيع الدولة التحكم فى بياناتها والمعلومات، التى تتدفق عبرها، ويكمن التحدي في بناء سيادة رقمية لا تُفهم على أنها سيادة رقمية فريدة؛ بل باعتبارها عالمًا رقميًا تتعايش فيه العديد من السيادات([1])، تمامًا كما تتعايش دول عدة على الأرض([2]).

ولذلك كان لازماً علينا فى عرضنا للسيادة الرقمية أن نحدد الأمور الآتية باعتبارها تشكل فى مجملها محددات للسيادة الدولة الرقمية.

**أولاً**: **الفضاء السيبراني**:

([1]) **سلاوي بشرى و أخرين**: مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة دراسة تحليلية استشرافية، كلية العلوم الإنسانية والاجتماعية، 2020، ص59.

([2]) **Pierre-Yves Quiviger**: Une approche philosophique du concept émergent de souveraineté numérique, Nouveaux Cahiers du Conseil constitutionnel n° 57 (dossier : droit constitutionnel à l'épreuve du numérique) - octobre 2017

**يعرف الفضاء السيبرانى Cyberspace**، بإعتباره الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت، وشبكات الاتصالات، وأنظمة الحاسب الآلي، والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرد([1]).

**وتُعرِّف الوكالة الفرنسية للأمن السيبرانى French Cybersecurity Agency** (ANSSI ) في سرد المصطلحات الخاص بها ، الفضاء السيبرني **Cyberspace** بأنه "مساحة اتصال تتشكل من الترابط العالمي لمعدات معالجة البيانات الرقمية "([2]).

**ووزارة الدفاع الأميركية**، على سبيل المثال، تعتبر الفضاء السيبرانى **Cyberspace** "مجالًا عالمياً ضمن بيئة المعلومات يتكون من شبكة مترابطة من البنى التحتية لتكنولوجيا المعلومات، بما في ذلك الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات وأجهزة التحكم المدمجة"([3]) ومن ناحية أخرى، تعرف

---

(1) ظهرت عبارة Cyber فى أعمال Norbert Weiner الذى قدم تعريفاً لعبارة Cybernetiecs فى منتصف القرن العشرين، مفادها أن التفاعل بين الأنسان والآلة يؤدى إلى خلق بيئة بديلة للاتصال تشكل البنى الأساسية لمفهوم الفضاء السيبرانى، وفى اوائل الثمانينات صاغ الكاتب William Gibson عبارة Cyber Space فى رواياته عن المستقبل؛ حيث وصف الفضاء بأنه هلوثة رضائية يمارسها ملايين البشر يومياً فى جميع الأوطان، وفى اوائل تسعينات القرن الماضى وضع John perry Barlow العبارة كمفهوم معاصر فى سياق وصفه للعلاقة بين الكمبيوتر وشبكات الاتصال السلكية واللاسلكية، وقد وصف الفضاء السيبرانى بأنه وطن بلا حدود، فالفضاء السيبرانى مجال افتراضى من صنع الانسان يعتمد بشكل أساسي على أنظمة الكمبيوتر وشبكات الإنترنت والكم الهائل من البيانات والمعلومات المعالجة الكترونياً. للمزيد راجع فاطمة بيرم، السيادة الوطنية فى ظل الفضاء السيبرانى والتحولات الرقمية: الصين نموذجاً، مرجع سابق، 792،
أنديرأعراجي، القوة في الفضاء السيبراني ؛ فصل عصري من التحدي والإستجابة، 2015، ص 12 وما بعدها.

**Norbert Wiener**: Cybernetics or control and communication in the animal and the machine, second edition, the Massachusetts Institute of Technology Press, Cambridge, England, 1984,

(2) **French Cybersecurity Agency** https://cyber.gouv.fr/en/french-approach-cyber-0

(3) cyberspace- A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Pub, J. (1994). Pub 1-02. Department of Defense Dictionary of Military and Associated Terms, 23.P:64

Cyberspace – interconnected and interdependent network of information technology infrastructures, including the Internet, telecommunications

**المفوضية الأوروبية** الفضاء السيبرانى بشكل غامض بأنه "الفضاء الافتراضي الذي يتم فيه تداول البيانات الإلكترونية لأجهزة الكمبيوتر الشخصية في جميع أنحاء العالم"([1]).

ويمكن أيضاً فهم هذا الأخير من خلال محتواه: فهو يجمع بين" جميع البيانات الرقمية (البرامج والمستندات النصية أو الصوتية أو المرئية) المتوفرة على الإنترنت والأجهزة و البنية التحتية للبرامج التي تمنحها الانتشار في كل مكان([2]).

**ويعرف الفضاء السيبرني Cyberspace** كونه " المجال أو الوسط الذي ينتج عن عملية الاتصال بين شبكات الإنترنت- عامةً كانت أو خاصة، عالمية كانت أو محلية، من طريق الحواسب الآلية والهواتف الذكية، بغرض إنشاء وتداول واستغلال ونشر والاحتفاظ بمحتوي رقمي، مصوراً كان أو مكتوباً - و مسجلاً، وسواء أكان هذا المحتوي الرقمي عبارة عن بيانات أو معلومات تمت معالجتها، وسواء أكانت لأغراض سياسية أو اقتصادية أو اجتماعية أو ثقافية أو غيرها، ويتكون هذا الفضاء من اجتماع عناصر مادية كأجهزة الكمبيوتر، والهواتف الذكية، وأخري غير مادية كأنظمة الشبكات والبرمجيات، وحوسبة المعلومات ونقل وتخزين البيانات ومنتجي ومستخدمي كل هذه العناصر([3]).

---

networks, computer systems, interconnected devices, embedded processors, and controllers

(1) **Rain Ottis, Peeter Lorents:** Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Webopedia, for example, offers a definition similar to the previous one, claiming that cyberspace is a “metaphor for describing the non-physical terrain created by computer systems”. (Webopedia) Even though they are similar, their usefulness is limited because of vague terminology and concepts. The Wikipedia, however, offers that cyberspace “is the global domain of electromagnetics as accessed and exploited through electronic technology and the modulation of electromagnetic energy to achieve a wide range of communication and control system capabilities.” (Wikipedia) Here we have a definition that includes the technology component, the human component (who accesses and exploits) and the communication and control component, which brings us back to Norbert Wiener’s definition of cybernetics

(2) **Vassilys Fourkas:** What is ‘cyberspace’? March, 2004, https://www.researchgate.net/publication/32892863

(3) ) **انظر د. حسين أحمد مقداد:** دور الضبط الإدارى في الحد من مخاطر الفضاء الإلكترونى فى مصر وفرنسا، مجلة العلوم القانونية والاقتصادية ، العدد الأول ، السنة الخامسة والستون ، يناير 2022، ص639

ويُعرّف خبير الأمن السيبراني **Daniel Kuehl** الفضاء السيبرانى بأنه "مجال عالمي داخل نظام المعلومات يتميز بطابعه المميز والفريد من خلال استخدام الإلكترونيات والطيف الكهرومغناطيسي لإنشاء وتخزين وتعديل وتبادل واستغلال المعلومات عبر شبكات مستقلة، ومترابطة باستخدام تقنيات المعلومات والاتصالات"([1]).

ويعّرف **فريدريك مايور** ذلك الفضاء السبيرني" بأنه بيئة إنسانية وتكنولوجية جديدة، للتعبير والمعلومات والتبادل، وهو يتكون أساسًا من الأشخاص الذين ينتمون لكل الأقطار والثقافات واللغات والأعمار والمهن المرتبطة ببعضها البعض عن طريق البنية التحتية التكنولوجيا، التي تسمح بتبادل المعلومات ونقلها بطريقة رقمية([2]).

وعليه تستخدم كلمة Cyber مقترنة بكلمة Space لتشير إلى أشهر تعبير فى عصر المعلومات واصبح هذا التعبير أشمل وأوسع من الإنترنت ليضم كل الأتصالات والشبكات وقواعد البيانات، ويشير كذلك إلى مجموعة المعلومات المتوفرة إلكترونياً، ويتم تبادلها وتشكيلها فى مجموعات بناء على استخدمها ([3]).

وعليه فاذا اعُتبر أن السيادة هي السلطة العليا للدولة على إقليمها، فأن أول تمييز هو أن الفضاء الرقمى ليس إقليماً حقيقياً، بل بنية تحتية عالمية، ومع ذلك يتم وصفها بشكل متزايد على أنها مساحة أو أقليم لجعلها فى متناول سيطرة الدولة هذا من ناحية .

ومن ناحية أخرى، فأن الدول القومية لا تتمتع بالسلطة المطلقة على البنية التحتية الرقمية، فالغالبية العظمى من الحالات ولا سيما فى الاتحاد الأوروبى وروسيا والصين تم اقتراح السيادة الرقمية كنوع من الإستراتيجية الدفاعية، التى تهدف إلى زيادة سلطة الدولة على البنية التحتية الرقمية، وخاصة على التقنيات الرقمية الأجنبية ( أى التقنيات الأمريكية)([4]) .

---

(1) **See Daniel T. Kuehl**: "From Cyberspace to Cyberpower: Defining the Problem," Cyberpower and National Security, (Washington, DC: Potomac Books, 2009),P 38.

([2]) للمزيد راجع:

Position Paper, On the Application of International Law in Cyberspace, 'Cyberspace' itself is understood here as the conglomerate of (at least partly interconnected) 'cyber infrastructures' and 'cyber processes' in the above-mentioned sense. In this paper, the adjective 'malicious', when used to describe certain activities in cyberspace, is not purported to carry a technical legal meaning, March 2021.

(3) **Rain Ottis, Peeter Lorents**: Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, p3.

**(4) Samuele Fratini:** Quels Sont Les Modèles De Mise En Œuvre De La Souveraineté Numérique ? op. cit. P 13

والفضاء السيبرانى فريد من نوعه من حيث أنه الفضاء الاستراتيجي الوحيد الذي أنشأته يد الإنسان، ليبدو هذا العالم غير المادي كعالم يجب غزوه أو على الأقل، ممارسة السلطة فيه.

**ويتكون الفضاء السيبرانى من ثلاثة طبقات:([1])**

**أولاً**: أنظمة البيانات التى هى جوهر السيادة الرقمية؛ وتعد البيانات والحصول عليها سمة من سمات القوة والسيادة بالنسبة للدول، وهى المادة الأولية للفضاء السيبرانى، وتنتج هذه البيانات نتيجة تراكم المعلومات المخزنة، نتيجة الأنشطة التى يقوم بها الافراد، ولذلك أدركت الشركات الكبرى إن التحدى الرئيسى يتمثل فى الوصول إلى هذه البيانات والتحكم فيها، ولذلك تستثمر الدول مبالغ طائلة فى هذه المادة والاستفادة منها.

**ثانياً**: أنظمة التطبيقات والبرامج التى تسمح بمعالجة البيانات؛ وتعتبر هذه الانظمة، هى محرك الفضاء السيبرانى فبدون معالجة هذه البيانات تظل غير ضرورية على الاطلاق ، ولكن معالجة هذه البيانات تتطلب خوادم ضخمة Servers وطاقة هائلة من أجل تخزينها، وهنا يكمن التحدى فتطبيقاً على ذلك نجد أن مجال التجارة والتسويق يسمح بمعالجة هذه البيانات من أجل التعرف على عادات المستهلكين، مما يسهل تقديم العروض للفئات المستهدفة، ولذلك اضحت أشكال معينة من تطبيقات الذكاء الاصطناعى، تشكل سمة من سمات قوة الدولة وقدرتها على فرض سياتها الرقمية([2]).

**ثالثاً**: الشبكات والاجهزة الكمبيوتر التى تسمح بالتبادل أو الاتصال الرقمى؛ وتسمى بالطبقة المادية أو البنية التحتية، وتضم كل المعدات والاجهزة الملموسة، وهذه البيانات والتطبيقات والأجهزة وحدات افتراضية، ولكى تتفاعل مع العالم الواقعى، تعتمد على الشبكات والخوادم، والحواسيب، وهذه منها ما هو موجود على الأرض كالخوادم، ومنها موجود فى البحر كالكابلات، ومنها موجود فى الفضاء الخارجى كالاقمار الاصطناعية، التى تعزز أنظمة الدفاع العسكرية فى دول عدة،

ويجدر الإشارة إلى أن الطبقات الثلاث مكملة لبعضها البعض، وسلامة هذه المكونات تساهم فى حماية البيانات والمعلومات الحساسة للدولة، وتقديم الخدمات الرقمية بشكل مستمر وموثوق به، مما يساهم فى بناء الثقة بين المواطنين والدولة، وتعزيز قوة الدولة وسيادتها الرقمية.

ولذلك، فإن السيادة الرقمية، التي تُفهم على أنها السلطة السياسية العليا التي تُمارس على إقليم ما، يجب أن تنطبق على هذه المستويات الثلاثة للفضاء السيبراني؛

---

([1]) **إيجر امنية:** السيادة الرقمية فى العالم المعولم: التحديات والرهانات، مجلة الدراسات القانونية والسياسية، الجزائر المجلد 10 عدد2 يونيو 2024 ، ص 76.

([2]) **See Madhuvanthi Palaniappan:** Cyber Sovereignty: In Search of Definitions, Exploring Implications, Issue Brief ISSUE NO. 602 December 2022, P 7

وإلا فإن رابط الأعتماد التكنولوجي سيكون موجودًا دائمًا. وبمعنى أخر، سيهيمن الكيان الذي يتحكم في طبقاته الثلاث على الفضاء الرقمي ويفرض سيادته على هذا الفضاء.

**خصائص الفضاء السيبرانى.**

يتميز الفضاء السيبرانى بمجموعة من الخصائص هى:

1) الفضاء السيبرانى فضاء غير منظم؛ والسبب فى ذلك يرجع كونه فضاء افتراضى، يجعل من الصعوبة وضع حدود لسيطره عليه، وفرض الدول سيادتها على هذا الفضاء، وعليه فغياب الحدود الجغرافية يسهل عملية انتقال الانشطة والمعلومات والتواصل فى كل وقت وأى مكان دون قيود زمنية ومكانية فى ظل ضعف القوانين الدولية، للسيطرة على هذا الفضاء مما يودئ إلى صعوبة الردع السيبرانى([1]).
2) الفضاء السيبرانى فضاء موحد؛ من حيث استخدام نفس الاجهزة والشبكات والكابلات والتكنولوجيا فى جميع المجالات، كالصحة والنقل والطاقة والدفاع، وهذا ما يجعله عرضه للهجمات والاختراقات، وهذا ما جعل كثير من الدول تسعى لتطبيق أنظمة، مثل البلوكتشين، لحماية مصالحها وضمان سلامة بياناتها الهامة.
3) الفضاء السيبرانى فضاء غير مؤمن بشكل كافى؛ فيواجه الكثير من التهديدات الامنية الكبيرة، مثل اختراقات إلكترونية كالهجوم الواقع على شركة مايكروسوفت، والاحتيال إلالكترونى والبرمجيات الخبيثة، التى تمثل جرائم سيبرانية، بالإضافة إلى الارهاب السيبرانى.
4) الفضاء السيبرانى فضاء فريد من نوعه؛ فهو المحرك للتحول الرقمى فى مختلف القطاعات، بما فى ذلك التعليم والصحة والاقتصاد، ويتدخل فى معظم أنشطة الحياة اليومية للأفراد([2]).
5) الفضاء السيبرانى فضاء استراتيجى؛ نظراً للمكانة المركزية التى جعلته ضمن الاستراتيجيات الوطنية الاقتصادية والاجتماعية لكثير من الدول، وجزء من استراتيجية الدولة الشاملة، إضافة إلى أنه اصبح ساحة جديدة للصراع الإلكترونى بين الدول.

**ثانياً: شركات تكنولوجيا المعلومات والاتصالات.**

إذا كان الفضاء السيبراني منطقة تتصادم فيها قوى الدولة، فإن جهات فاعلة جديدة من القطاع الخاص تطبق قوتها هناك أيضاً، ولذلك فإن إثبات سيادة هذه الشركات الرقمية أمر أكثر تعقيدًا. ويبدو أن السيادة، التي كانت مرتبطة تقليدياً بالدولة،

---

(1) **Grégoire Germain et Paul Massart:** Souveraineté Numérique, Revue Études, N° 10 , Octobre 2017, Pp.45 À 58.
https://Www.Cairn.Info/Revue-Etudes-2017-10-Page-45.Htm

(2) Cyberspacs Operations, Joint publication 3-12 (R) 5 February 2013.

غير متوافقة مع كيان خاص. ومع ذلك، فإن ثقلها في العالم الرقمي يقودها إلى أن تصبح ذات سيادة.

فالتحكم في البيانات الرقمية الناتجة عن أنشطة 4.5 مليار مستخدم متصل قابلين للزيادة كل ثانية، يضاف إلى حالة الأحتكار الأفتراضي لبعض الشركات الأمريكية خاصة (GAFAM و NATU- Netflix، Airbnb، Tesla، Uber) بالإضافة إلى (BATX الصينية أو Yandex محرك البحث الروسية) ، يمنح هؤلاء المشغلين قوة تتضاهى أن لم تكن تتفوق على السلطة المقررة من جانب الدولة لفرض سيادتها على مواطنيها([1]).

هذه الشركات هي اليوم أمريكية بشكل رئيسي، على الرغم من أنه من الضروري أن نأخذ في الاعتبار شركات من دول ثانية، حتى لا يقتصر موضوع السيادة الرقمية على "الحرب الباردة الرقمية"، في معارضة سياسية بسيطة بين الاتحاد الأوروبي والصين والولايات المتحدة.

**ولكن هنا يثار تساؤل هام، وهو ماذا تمثل سيادة هذه الشركات؟** من الممكن هنا التواصل مع تفكير Annie Blandin-Obernesser الذى تقترح تصنيف الشركات التي تمتلك قوة سوقية على أنها ذات سيادة، بحيث تزود نفسها بصفات السيادة والسلطة الحقيقية للحكومة([2]).

كما يمكن القول أيضًا، أن هناك مقاربة ثانية ذات طبيعة سياسية واقتصادية: فالسيادة الرقمية ستكون عندئذٍ للمشغلين الاقتصاديين (GAFAM) الذين لديهم في الواقع سلطة فرض قواعدهم على المستفيدين من خدماتهم، ويتمتع عدد قليل من الشركات متعددة الجنسيات بهذا التفوق، وذلك بفضل هيمنتها في الأسواق، وممارسة سلطة حقيقية للقيادة والتنظيم في الفضاء الإلكتروني.

---

(1) إذ يصل حجم الأشخاص، الذين يستخدمون شبكة الفيسبوك، إلى ما يفوق المليارى شخص، ويصل العدد إلى 800 مليون، على انستغرام، وإلى أكثر من مليار على واتساب، يتجاوز حجم البيانات التي تنتج عن هذا الاستخدام، 2.5 إكسا بايت ExaByteفي الدقيقة الواحدة تقريبًا، وتعتبر تطبيقات المحادثات الفورية، مصدرا أخر لإنتاج البيانات حيث يتم إرسال أكثر من 527 ألف صورة، بواسطة السناب شات، في الدقيقة، وتحصل منصّة Linked in على أكثر من 120 حساب جديد، ويرسل مستخدمو تويتر 456 ألف تغريده، بينما يُعالج جوجل أكثر من 3.6 مليون عملية بحث، وتجني أمازون أكثر من ثلاثمائة ألف دولار أمريكي من المبيعات، التي تجري في الدقيقة الواحدة على الإنترنت، هذا، بالأضافة إلى الحجم الهائل للاستثمارات، التي تقوم بها الدول في مجال البيانات الضخمة. راجع د. منى الأشقر جبور ، ود محمود جبور: البيانات الشخصية والقوانين العربية: - الهمّ الأمني وحقوق الأفراد، المرجع السابق، ص 14.

(2) **Annie Blandin-Obernesser**: Les entreprises souveraines de l'Internet : un défi pour le droit en Europe., Droits et souveraineté numérique en Europe, Bruxelles, Bruylant, à la p 95

وبالتالي، فإنهم يضعون الشروط العامة لأستخدام الخدمات عبر الإنترنت، التي أصبحت ضرورية، ويطورون خوارزميات، ويقررون حذف المحتوى، وإغلاق ملف تعريف المستخدم، والاحتفاظ بالبيانات الشخصية التي يخزنها أو بيعها، إضافة إلى انها تنشئ البعض منها عملات افتراضية خاصة بها، مثل( Bitcoin,Tether USDt Ethereum,)، وإنشاء خدمات تسوية المنازعات الخاصة به.

والشركات الاتصالات يمكن أن تساعد فى التصدى للجهمات السيبرانية([1])، إضافة إلى إن لديها القدرة على وضع القواعد والمعايير الخاصة بها، والتى تتطلب من هذه الشركات أن تقوم بفكرة التنظيم الذاتى؛ وهى فكرة تقوم على وضع قواعد وسلوكيات ذاتية، لتنظيم أنشطتها وأعمالها بدلاً من الاعتماد على القوانين واللوائح الحكومية المحلية والدولية، والهدف منها، هو تحقيق التوازن بين تحقيق الأرباح والمسؤولية الاجتماعية والبيئية، وتعزيز الممارسات الأخلاقية لدى هذه الشركات([2]).

ومن خلال التنظيم الذاتي، لهذه الشركات تستطيع بناء سيادية رقمية، بناء على معايير خاص بها في الفضاء السيبراني. ومع ذلك، فإن علامة سيادتها لا تتمثل في بناء مساحة قانونية خاصة منفصلة فحسب، بل في القدرة على تطبيق هذه القواعد مع الدول، التى تستخدم منصات هذه الشركات حتى ولو كان تطبيق هذه القواعد بصورة تفاوضية، وتتجلى هذه القوة التفاوضية بشكل خاص في تطبيق قانون البيانات الشخصية، ومثال على هذا ما تم التفاوض بشأنه على فترة الاحتفاظ بالبيانات الشخصية بين شركة Google والمفوضية الأوروبية، للتوصل إلى حل وسط بين توصيات المجموعة 29 وممارسات Google وكانت مجموعة المادة 29 تقترح أن تكون فترة الاحتفاظ بالبيانات الشخصية من قبل موفري محركات البحث ستة أشهر، وتفاوضت شركة Google التي اختارت فترة احتفاظ مدتها ثمانية عشر شهراً، مع المفوضيةالأوروبية لفترة احتفاظ أطول، وتم تحديد الموعد النهائي أخيراً في اثني عشر شهرًا.

---

([1]) Consciente de l’impact croissant des grandes entreprises sur le cyberespace mondial, l’étude appelle le secteur privé à une plus grande responsabilité dans la gestion des cyberattaques, en s’abstenant de pirater et en s’abstenant de développer ou de maintenir des produits TIC dont les défauts de conception ou le support inadéquat pourraient avoir des effets systémiques. Ces efforts en faveur d’une plus grande responsabilité ont été transposés dans des discussions formelles et même des engagements lors de la réunion du Forum mondial de l’OCDE de décembre 2018, qui doit être suivie prochainement. L'approche française du cyberspace, Publié le 03 octobre 2023 Mis à jour le 28 novembre 2023, https://cyber.gouv.fr/en/french-approach-cyber-0

([2]) **سلاوي بشرى و أخرين**: مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة دراسة تحليلية استشرافية، مرجع سابق، ص59.

إضافة إلى ذلك، تكمن قوة هذه الشركات في تطبيق القانون داخل الحدود الوطنية، مما يؤدي في بعض الأحيان إلى تراجع دور القاضى الوطنى فى تطبيق القانون، ومثال على هذه الحالة ما تم تكريسه فى ضوء الحق في إلغاء الإشارة الذي أقره حكم Spain Google الصادر في 13 مايو2014، والذى من خلاله يمكن لمستخدمي الإنترنت طلب تطبيق الحق في النسيان الرقمي على أساس المادة 14 تنص من التوجيه 46/95، "حق صاحب البيانات في الاعتراض"، على ما يلي: "تمنح الدول الأعضاء لصاحب البيانات الحق في: الاعتراض في أي وقت على أسباب مشروعة مقنعة تتعلق بوضعه الخاص على معالجة البيانات المتعلقة به، ما لم ينص التشريع الوطني على خلاف ذلك. وفي حالة وجود اعتراض مبرر، لا يجوز أن تشمل المعالجة التي بدأها المتحكم تلك البيانات".([1]).

ولكن تطبيق هذا الحق الجديد على المواطنين الأوروبيين يقع في أيدي محرك البحث، الذي يحدد ما إذا كان هذا الطلب يتفق مع القواعد المنظمة لهذا الحق، ومتفق مع النموذج الذي وضعته Google كما لا يمكن لشخص أن يملك حق المعارضة، وفي حالة رفض طلبه يمكنه اللجوء إلى القاضى الوطنى.

ولتعزيز سيادة بعض الشركات بدأت في ممارسة خدمات تشابه فى دورها مع الخدمات العامة التى تقدمها الدولة، والذى ساعد هذه الشركات هو الاعتراف بحقوق الإنسان على شبكة الإنترنت، إلى جانب تزايد إضفاء الطابع الذاتي على الحقوق، يميل إلى منح اللاعبين الرقميين دوراً عاماً في الدفاع عن الحريات الفردية. وتظهر بعض المنصات، كخدمات شبه عامة من خلال البديل الذي تقدمه للمهام التي تقوم بها الدولة التقليدية([2]).

---

**(1) Google Spain SL and Google Inc. v Agencia Española** de Protección de Datos (AEPD) and Mario Costeja González.

Article 14 of Directive 95/46, entitled ‘The data subject’s right to object’, provides: ‘Member States shall grant the data subject the right:

at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data

**([2]) N. Lucchi** "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011.

فمحركات البحث المجانية، والوصول إلى التوثيق والمعرفة وقدرات التخزين والحساب المتزايدة باستمرار تجعل الإنترنت منافساً للعديد من الخدمات العامة، سواء التعليم أو السلامة أو الصحة.

وبالمثل، يلعب مشغلو الاتصالات دوراً رئيسياً في احترام حرية الوصول إلى الإنترنت، والوصول إلى الشبكة دون تمييز، وهوما نجد آثاراً له في دليل حقوق الإنسان لمستخدمي الإنترنت، وتحمل هذه القدرة على تنظيم الشبكة نقاشاً قديماً حول حيادية الإنترنت. وفي السياق نفسه، يمكن الاعتراف بأن الشبكات الاجتماعية لها دور في النقاش الديمقراطي: ففي الولايات المتحدة، اعترفت المحكمةالعليا في 19 يونيو 2017 بأن الوصول إلى الشبكات الاجتماعية كان حقاً دستوريا([1]).

وتشهدالقدرة التنظيمية لهؤلاء اللاعبين الرئيسيين على قوتهم في العالم الرقمي. ويمكن الاعتراف بهم كسيادة عندما تكون قوتها الاقتصادية تسمح لها بتنفيذ سياستها، وتطبيق قانونها على الدول، فمشكلة التطبيق خارج الحدود الإقليمية، ويقصد بالتطبيق خارج الحدود الإقليمية الحالة التي تحكم فيها سلطات الدولة (التشريعية أو التنفيذية أوالقضائية) العلاقات القانونية القائمة خارج تلك الدولة، وهذا التطبيق يتجاوز الحدود الإقليمية، لأنه يطبق قانون دولة واحدة، في أغلب الأحيان الولايات المتحدة.

وبينما تخضع معظم الأنشطة البشرية الآن للتكنولوجيات الرقمية ، دخلت الدول في صراع على السلطة مع الشركات متعددة الجنسيات التي تهيمن على الشبكات الرقمية، فمسألة الحفاظ على السيادة الرقمية للدول فى الفضاء الرقمى، أو استعادة جزء من السلطة التي تمارس في هذه المساحات الجديدة، على الرغم من تصورها للهروب من قبضة الدولة، جعلت التكريس لسيادة الدولة الرقمية أمر ضروريًا.

**رابعاً:الأفراد.**

---

([1]) **Packingham V. North Carolina**, No. 15–1194. Argued February 27, 2017—Decided June 19, 2017." A fundamental First Amendment principle is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more. Today, one of the most important places to exchange views is cyberspace, particularly social media, which offers "relatively unlimited, low-cost capacity for communication of all kinds," Reno v. American Civil Liberties Union, 521 U. S. 844, 870, to users engaged in a wide array of protected First Amendment activity on any number of diverse topics. The Internet's forces and directions are so new, so protean, and so far reaching that courts must be conscious that what they say today may be obsolete tomorrow. Here, in one of the first cases the Court has taken to address the relationship between the First Amendment and the modern Internet, the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium.

يُعد الفرد هو العنصر الفعال في السيادة الرقمية، فهو الذي يقدم بياناته ومعلوماته، ويسمح بنقلها على الشبكة، ولذلك لكل مواطن الحق في الوصول لكل المعلومات المحوسبة المتعلقة به، وطلب تصحيحها وتعديلها، وأن يُبلغ بالغرض منها، وكل ذلك على النحو المنصوص عليه في القانون([1]).

ولهذا لا يجوز وفقاً للائحة العامة للبيانات الأوروبية RGPD استخدام الحواسب لمعالجة بيانات تتعلق بالقناعات الفلسفية أو السياسية، أو الانتماءات الحزبية أو النقابية، أو المعتقدات الدينية، أو الحياة الخاصة أو الأصول العرقية، إلا بموافقة الشخص موضوع البيانات، أو بإذن ينص عليه القانون، وينطوي على ضمانات بعدم التمييز، أو بغرض معالجة بيانات إحصائية لا يمكن الوقوف على هوية الأفراد المكوّنين لها، ويُحظر حصول طرف ثالث على البيانات الشخصية إلا في الحالات الاستثنائية التي ينص عليها القانون([2]).

وهذا ما يطلق علية سيادة المستخدم أو المستهلك"user sovereignty" ([3]) والذى تعنى ضرورة التأكيد على حماية سيادة الأفراد بإعتبارهم مستهلكين للخدمات

---

(1) Le règlementvient apporter sa pierre à l'édifice de la souveraineté individuelle en renforçant le consentement des individus ainsi qu'en affirmant de nouveaux droits de l'individu dans l'univers numérique), Marin Brenac: La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique,(86-90),U.Laval Québec,Canada, 2017

([2]) Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité. Le droit à la protection des données à caractère personnel n'est pas un droit absolu; il doit être considéré par rapport à sa fonction dans la société et être mis en balance avec d'autres droits fondamentaux, conformément au principe de proportionnalité. Le présent règlement respecte tous les droits fondamentaux et observe les libertés et les principes reconnus par la Charte, consacrés par les traités, en particulier le respect de la vie privée et familiale, du domicile et des communications, la protection des données à caractère personnel, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté d'entreprise, le droit à un recours effectif et à accéder à un tribunal impartial, et la diversité culturelle, religieuse et linguistique, Règlement (Ue) 2016/679 Du Parlement Européen Et Du Conseil.

**([3]) Julia Pohle:** Digital sovereignty A new key concept of digital policy in Germany and Europe, Konrad-Adenauer-Stiftung e. V. Berlin. 2020,P18

الرقمية([1])، ولهذا احتوى ميثاق سيادة المستهلك فى العالم الرقمى الذى نشرته وزارة الأغذية والزراعة وحماية المستهلك عام 2007 على أهمية أمن تكنولوجيا المعلومات كضمانة أساسية لحق تقرير المصير المعلوماتى، ولذلك ترتكز حماية سيادة الأفراد (المستخدم) على فرصهم ومهاراتهم فى الاستفادة من التقنيات الرقمية بشكل مستقل ومسئول، وهذا ما عرفه المجلس الاستشارى لقضايا المستهلك عام 2017 بأن سيادة المستخدم" هى القدرة على التصرف بحرية فى اختياراتهم وتولى أدوار مختلفة فى العالم الرقمى"([2]).

من هذا المنطلق تكون مسألة السيادة الرقمية للمستخدمين. منبثقة من أسس السيادة الشعبية، التي يعتبر المواطنون بموجبها مصدر كل سلطة، وتتوافق مع حق الشعب في تقرير المصير. ويمكن للمستخدمين الاختيار، والتعبير عن التفضيلات الخاصة بهم، والابتعاد عن تطبيقات معينة، فقد اختلفت حياة الأفراد فى ظل الانفتاح غير المحدود للعالم الرقمى، الأمر الذى جعل الفرد ذاته مادة محورية لهذا العالم من خلال البيانات والمعلومات المتعلقة به([3]).

ولهذا وفي ظل ظروف المعالجة الحديثة للبيانات، تعتمد حماية الفرد من جمع بياناته الشخصية، وتخزينها واستخدامها والكشف عنها بشكل غير محدود على الحق الشخصي العام المنصوص عليه في المادة 2 الفقرة 1 ط .V .مع المادة 1 الفقرة 1 ز. وفي هذا الصدد، يضمن الحق الأساسي حق الفرد في أن يقرر بنفسه الكشف عن بياناته الشخصية واستخدامه، ولا يجوز فرض قيود على هذا الحق في "تقرير المصير المعلوماتي" إلا لتحقيق المصلحة العامة العليا. فهي تتطلب أساسًا قانونيًا دستوريًا يجب أن يتوافق مع متطلبات سيادة القانون المتمثلة في وضوح القواعد.

---

([1]) **احمد محمد محمد عبد الغفار:** مبدأ السيادة الرقمية الفردية على البيانات، مجلة البحوث الفقهية والقانونية، العدد 43، كلية الشريعة والقانون، جامعة دمنهور، 2023، ص 785.

([2]) defined digital sovereignty as the consumers' ability to act and as his/her freedom of choice to assume different roles in the digital world, i. e., as market participants, consumercitizens of a society as well as 'prosumers' in social networks, Digitale Souveränität Gutachten des Sachverständigenrats für Ver braucherfragen,(Digital Sovereignty Report of the German Expert Council for Consumer Affairs) SVRV, 2017,P3

([3]) **محمد عرفان الخطيب:** ضمانات الحق في العصر الرقمي من تبدل المفهوم .. لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويتي، المرجع السابق، ص256.

وعند وضع اللوائح، يجب على الهيئة التشريعية أيضًا مراعاة مبدأ التناسب. ويجب عليه أيضًا، اتخاذ الاحتياطات التنظيمية والإجرائية لمواجهة خطر انتهاك الحقوق الشخصية([1]).

وهذا ما نص علية الدستور اليونانى فى مادته 9 أ حيث قرر أن" يحق لكل شخص أن يتمتع بالحماية من جمع ومعالجة واستخدام بياناته الشخصية، وخاصة بالوسائل الإلكترونية، على النحو الذي يحدده القانون. ويتم ضمان حماية البيانات الشخصية من قبل هيئة مستقلة، يتم تشكيلها وتشغيلها على النحو الذي يحدده القانون"([2]).

ومن هذا الحكم انطلق حق تقرير المصير المعلوماتى الذى يستخلص منه حق الفرد فى سيادته على بياناته الشخصية المعالجة الكترونية، إلى دول الاتحاد الأوروبى حتى استقر ضمن الحقوق الأساسية، فى أطار المبادئ العامة لمحكمة العدل الأوروبية، التى اقرت حق الشخص المعنى بالبيانات فى التحكم فى الافصاح عنها أو محوها من محركات البحث والمعروف حالياً بحق النسيان الرقمى([3])([1]).

---

(1) Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikel 2 Abs. 1 i. V. mit Artikel 1 Abs. 1 GG umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

- Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei der Regelung hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken. (Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983)

(2) **Art 9** A All persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law. The protection of personal data is ensured by an independent authority, which is constituted and operates as specified by law

([3]) **عبد الهادى فوزى العوضى:** الحق فى الدخول فى طى النسيان على شبكة الإنترنت، دراسة قانونية تطبيقية مقارنة، دار النهضة العربية، 2014.

إلى جانب ذلك جاءت المادة 16 من اللائحة العامة لحماية البيانات بحق صاحب البيانات فى الحصول من المتحكم دون تأخير غير مبرر على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به، مع الأخذ في الاعتبار أغراض المعالجة، كما يحق له أيضاً، استكمال البيانات الشخصية غير المكتملة، بما في ذلك عن طريق تقديم بيان تكميلي([2]).

---

_ **مها رمضان محمد بطيخ:** الإطار القانوني للحق في النسيان عبر شبكة الإنترنت، مجلة الدراسات القانونية العدد الحادى والستون – الجزء الاول – يونيو 2020، ص216.

(1) On a proper construction of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and of Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 (General Data Protection Regulation), where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request. Judgment of the Court (Grand Chamber) of 24 September 2019.Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL).Request for a preliminary ruling from the Conseil d'État, Reference for a preliminary ruling— Personal data— Protection of individuals with regard to the processing of such data— Directive 95/46/EC— Regulation (EU) 2016/679— Internet search engines — Processing of data on web pages — Territorial scope of the right to de-referencingCase C-507/17.

(2) La personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes. [2] Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

ويقرر البعض أن حق الفرد فى حرمة الحياة الخاصة لا يتعلق فقط بنطاق المسائل الشخصية التى حجبها عن الأخرين، ولا بالحق فى أن يتخذ اكثر قراراته اتصالاً بمصيره، وأشملها تاثيراً فى أنماط الحياة التى يفضلها ، ولا بالعلائق الزوجية وما هو صميم من روابطها، بما يعينها على النماء والتكامل ويكفل وحدتها، ولا بمعلوماته التى يتلقاها أو يحوزها فى شأن أخص الروابط وألصقها بدخائل نفسه، ذلك أن حق الناس جميعهم فى حرمة خواص حياتهم مفهوم عام يتناولها من أقطارها كافة، ليشمل كل ما ينبغى كتمانه منها فى نطاق توقعهم المشروع، فلا تتسلقها الدولة زحفاً عليها بما يقوض أكثر العلائق الشخصية عمقاً وتفانياً، ويهدر القيم الخلقية التى تحيط بالحياة، وتكفل دوامها واستقراراها([1]).

نتيجة لهذا يقول البعض أن السيادة الرقمية سواء كانت لشخص واحد أو جماعة فأن ترسيخ فكرة السيادة الرقمية يكون من خلال تفويض هذه السيادة إلى الجهات الفاعلة فى الدولة التى لديه السلطة على الشبكات الرقمية، هذا التفويض يجد أساسه فى الموافقة الأفراد فى معالجة بياناتهم، وهذا ما تساهم به اللأئحة الأوروبية لحماية البيانات الشخصية([2]).

ومن منطلق تعزيز حماية بيانات الشخصية وحقه فى التحكم فى بياناته ومعلوماته، صرحت محكمة النقض المصرية بأنه" إذ كان من المتعارف عليه أنه

---

[1] **د. عوض المر:** الرقابة القضائية على دستورية القوانين فى ملامحها الرئيسية ، مركز رينيه جان دبوى للقانون والتنمية بفرنسا، 2003 ، ص 1214

[2] Le renforcement des souverainetés individuelles et collectives par le règlement La souveraineté numérique conduit à une délégation de souveraineté aux acteurs les mieux à mêmes de répondre auxlo giques de réseaux du numérique. Au sein de ces acteurs se trouventen premier lieu l'individu, acteur le plus bas, car premier utilisateurdes services en ligne. On en vient à parler pour cet acteur d'unesouverai neté individuelle sur ses données personnelles, par le renforcement de sa capacité à contrôler l'usage qui en est fait. Lasouveraineté individuelle s'inscrit bien dans l'idée de délégation desouveraineté par l'État de la souveraineté numérique. Le règlementvient apporter sa pierre à l'édifice de la souveraineté indi viduelle en renforçant le consentement des individus ainsi qu'en affirmant de nouveaux droits de l'indivi du dans l'univers numérique), Marin Brenac: La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du conceptémergent de souveraineté numérique, op,cit,(86-90), Stefanie-Daniela Waldmeier: Informatio nelle Selbstbestimmung-ein Grundrecht im Wandel? Dissertation der Rechtswissenschaftlichen Fakultät der Universität Zürich zur Erlangung der Würde einer Doktorin der Rechtswissenschaft, Zürich, M.2015.

توجد مناطق من الحياة الخاصة لكل فرد تُمثل أغوارًا لا يجوز النفاذ إليها وهذه المناطق من خواص الحياة ودخائلها وينبغي دومًا _ ولاعتبار مشروع _ ألا يقتحمها أحد ضمانًا لسريتها وصونًا لحرمتها ودفعًا لمحاولة التلصص عليها أو اختلاس بعض جوانبها" وفى تعرضها لما يمثل انتهاك لبيانات الاشخاص تقرر" وبوجه خاص من خلال الوسائل العلمية الحديثة، التي بلغ تطورها حدًا مذهلًا، وكان لتنامي قدراتها على الاختراق أثرٌ بعيدٌ على الناس جميعهم حتى في أدق شئونهم وما يتصل بملامح حياتهم بل وبياناتهم الشخصية، والتي غدا الاطلاع عليها والنفاذ إليها كثيرًا ما يُلحق الضرر بأصحابها؛ إذ إن البشرية لم تعرف في أي وقت مضى مثل هذا التزايد الحالي والسرعة في العلاقات بين الناس، فبعد التلغراف والتليفون والراديو والتليفزيون كانت شبكة المعلومات والاتصالات الدولية المعروفة باسم الإنترنت، والتي ساهمت بشتى السبل في نقل وتبادل المعلومات بحيث تسمح بالتعرف الفوري على المعلومة والصورة والصوت والبيانات عبر أنحاء العالم لدرجة يمكن معها القول بتلاشي فروق التوقيت، فالإنترنت أصبح أداة جديدة للمعلوماتية والاتصال، وبذلك فهو يمثل ثورة في الاتصال الإلكتروني، وبهذا التطور السريع جدًا في نقل وتبادل المعلومات أصبح مجتمع القرن الحادي والعشرين هو مجتمع المعلومات، وفي هذا المجتمع ألغت سرعة سير وانتقال المعلومات الزمان والمكان وفسحت المجال أمام الحريات بحيث أصبح لكل شخص يعيش على أرض المعمورة الحق في الاتصال بغيره وتبادل الأفكار والمعلومات معه، وقد تدعم ذلك بصيرورة حق الاتصال والحصول على المعلومات وتداولها ليس فقط حقًا دستوريًا بل أيضًا حقًا من حقوق الإنسان وحرياته الأساسية إلا أن هذه التجربة الجديدة (الإنترنت) أظهرت من الخوف بقدر ما أظهرت من الإعجاب، وكان منبع الخوف قادمًا من أن الإنترنت ليس له حدود ولا قيادة قانونية، وبعبارة أخرى ليس له شخصية قانونية معنوية تمثله في مواجهة المستعملين له أو في مواجهة الغير؛ لأنه عبارة عن اتحاد فيدرالي للشبكات في مجموعها يغطي تقريبًا كل الكرة الأرضية، وكان مما لاشك فيه أن بحث الحماية القانونية ضد هذه الأخطار لا يكون إلا من خلال القانون والذي تطور في هذا المجال بوضع القواعد القانونية التي تحمي اعتداء أي شخص على الحياة الخاصة للآخرين من خلال الإنترنت؛ إذ أصبحت الحياة الخاصة في غالبية دول العالم قيمة أساسية تستحق الحماية"([1])، وقد أكدت هذه القيمة المادة 57 من الدستور المصري الحالي فنصت على أن "للحياة الخاصة حرمة، وهي مصونة لا تمس".

ولهذا فالسيادة الرقمية للأفراد مفهوم يعكس قدرة الأفراد على التحكم الكامل في بياناتهم الشخصية وهويتهم الرقمية على الإنترنت، بالإضافة إلى اتخاذ القرارات بشأن كيفية استخدام تلك البيانات ومن يمكنه الوصول إليها. في ظل التوسع الكبير في

([1]) **حكم محكمة النقض المصرية:** الطعن 9542 لسنة 91 ق جلسة 16 / 3 / 2022 مكتب فنى 73 ق 63 ص 507.

التكنولوجيا الرقمية واستخدام الإنترنت، أصبحت السيادة الرقمية موضوعًا مهمًا لمواجهة التحديات المرتبطة بالخصوصية، الأمان، والحقوق الرقمية.

ولهذا نقول أن السيادة الرقمية تفاعل بين ثلاث عناصر رئيسية هما؛ الفضاء السيبرانى الذى يشمل البنية التحتية العالمية، ويتم فيه جمع البيانات وتداولها واستخدمها، والشركات التكنولوجية التى تتحكم فى المنصات والخدمات التى تقدم للأفراد، ولها دور كبير فى تحديد كيفية استخدام البيانات، والأفراد المصدر الرئيسى فى للبيانات في الفضاء السيبرانى.

## المطلب الثانى

## التنظيم القانوني لتعزيز سيادة الدولة الرقمية.

تباينت العديد من الدول فى ترسيخها لفكرة السيادة الرقمية، سواء فى نصها على هذا فى دساتيرها – بصورة مباشرة أو غير مباشرة_ أو القوانين التى من خلالها تعمل الدول على فرض رقابتها على المعلومات والبيانات الخاصة بها، التى يتم تداولها فى الفضاء السيبرانى.

وحماية الفضاء السيبراني وبسط سيادة الدولة على مجالها الرقمى، أصبحت قضية هامة في دساتير العديد من الدول، خاصة في ظل التهديدات المتزايدة للأمن السيبراني([1]). مع ذلك، لا تشير معظم الدساتير بشكل مباشر إلى "الفضاء السيبراني"، ولكن العديد منها يتضمن نصوصًا تتعلق بحماية المعلومات، والخصوصية، والأمن الرقمي، أو الحقوق السيبرانية. وفيما يلي بعض الأمثلة:

من الدساتير التى نصت بصورة غير مباشرة دستور المانيا فى المادة العاشرة منه على حماية سرية المراسلات والاتصالات([2])، ودستور الولايات الولايات المتحدة

([1]) **أنديراَعراجي:** القوة في الفضاء السيبراني ؛ فصل عصري من التحدي والإستجابة، المرجع السابق، ص 76.

([2]) **Art10**" (1)- The privacy of letters as well as the secrecy of post and telecommunication are inviolable. (2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves the protection of the free

الامريكية لا يحتوي على نص صريح بشأن الفضاء السيبراني، لكنه يحمي الخصوصية الرقمية من خلال التعديل الرابع (Fourth Amendment)، الذي يمنع التفتيش والمصادرة غير المبررة، وهو ما يفسر اليوم على أنه يشمل البيانات الرقمية([1]).

ومنها أيضاً دستور إستونيا التى تعتبر من الدول الرائدة في الأمن السيبراني، ففي عام 2007، تعرضت إستونيا لهجوم سيبراني واسع النطاق استهدف البنوك، والوزارات، والبنية التحتية الرقمية، ودفع هذا الهجوم إستونيا لتكون في طليعة الدول، التي تطور قوانين وتشريعات قوية لتعزيز سيادتها الرقمية، وعلى الرغم من أن دستورها لا يشير مباشرة إلى حماية الفضاء السيبراني، وجاء فى المادة 16 منه أن لكل إنسان الحق فى حرمه حياتة الخاصة والعائلية ولا يجوز للوكلات الحكومية والسلطات المحلية ومسؤوليها التدخل فى الحياة الخاصة أو العائلية لأى شخص، إلا فى الحالات ووفقاً لإجراء ينص القانون عليه وذلك لحماية الصحة العامة أو الاخلاق العامة أو النظام العام، أو حقوق وحريات الآخرين([2])، ولكن نظامها التشريعي يتضمن قوانين واسعة لحماية البنية التحتية الرقمية والحقوق السيبرانية وهذه القوانين هى:.

- ❖ قانون الأمن السيبراني (Cybersecurity Act): والذى يُنظم إدارة وحماية البنية التحتية الحيوية الرقمية في إستونيا، ويفرض على المؤسسات الحكومية والشركات التي تدير البنية التحتية الأساسية (مثل الطاقة، الاتصالات، والتمويل) الالتزام بمعايير صارمة لحماية أنظمتها من الهجمات السيبرانية، إضافة إلى أنه يحدد مسؤوليات مشغلي البنية التحتية لتبني تدابير وقائية والتبليغ عن الحوادث السيبرانية.

---

democratic basic order or the existence or security of the Federation or a State [Land], the statute may stipulate that the person affected shall not be informed and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.

([1]) **Fourth Amendment** "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

([2]) **Art 26**. Everyone is entitled to inviolability of his or her private and family life. Government agencies, local authorities, and their officials may not interfere with any person's private or family life, except in the cases and pursuant to a procedure provided by law to protect public health, public morality, public order or the rights and freedoms of other, The Constitution of the Republic of Estonia, Entry into force 03.07.1992.

- ❖ قانون حماية البيانات (Data Protection Act): والذى يهدف إلى حماية خصوصية بيانات المواطنين، متماشياً مع لوائح الاتحاد الأوروبي مثل اللائحة العامة لحماية البيانات (GDPR)، وينظم كيفية جمع ومعالجة وتخزين البيانات الشخصية من قبل المؤسسات العامة والخاصة فى الدولة.
- ❖ مركز الدفاع السيبراني التابع للناتو The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub (CCDCOE): في عام 2008، استضافت إستونيا مركز التميز للدفاع السيبراني التابع لحلف شمال الأطلسي (الناتو) في عاصمتها تالين والذى يُركز على الأبحاث، والتدريب، ووضع استراتيجيات الدفاع السيبراني للدول الأعضاء في الناتو، ويُعد مرجعًا عالميًا لتطوير أفضل الممارسات والقوانين السيبرانية، التى تلجأ إليها الدول.
- ❖ برنامج الهوية الرقمية: إستونيا تُعد الدولة الأولى التي تقدم هوية رقمية شاملة لجميع المواطنين والمقيمين لديها، وتعتمد على بنية تحتية آمنة تدعم التوقيع الإلكتروني، والوصول إلى الخدمات الحكومية، والمعاملات المالية. وكذلك القوانين المرتبطة التى تضمن حماية البيانات، والأنظمة المستخدمة في هذا البرنامج من الاختراقات.
- ❖ الاستراتيجية الوطنية للأمن السيبراني: وضعت إستونيا استراتيجيات متعددة لتعزيز الأمن السيبراني، تشمل التعاون الدولي، والتدريب على مواجهة الهجمات السيبرانية، واستخدام التكنولوجيا الحديثة. وتشمل هذه الاستراتيجية إعداد فرق استجابة سريعة للحوادث السيبرانية (CERT).

إلي جانب ذلك نجد دستور الصين لا ينص صراحة على الفضاء السيبراني، لكن الحكومة الصينية أصدرت "قانون الأمن السيبراني" (2016)، الذي يعزز حماية البنية التحتية الحرجة، ومراقبة الفضاء السيبراني، وكذلك البرازيل الذى أُقرت "Marco Civil da Internet"، وهو إطار قانوني لحماية حقوق مستخدمي الإنترنت، كجزء من التشريعات المكملة للدستور التى تحمى من خلالها الفضاء السيبرانى وتعزز من سيادتها الرقمية.

وفى الدستور المصري تنص مادته الحادية والثلاثون على أن "أمن الفضاء المعلوماتى جزء أساسي من منظومة الأمن القومي"، مما يجعل مصر من الدول القليلة التي تذكر الأمن المعلوماتى صراحة فى الدستور وتعزز من سيادتها الرقمية.

ولهذا أصبحت السلطات العامة تدرك سرعة الحاجة إلى تنظيم المعالجة الحاسوبية للبيانات المتعلقة بنشاطها السيادى؛ المتضمن المرافق العامة والبنية التحتية الرقمية لديها و كذلك البيانات المتعلقة بالأشخاص الطبيعيين لديها، الأمر الذى جعلها في وقت مبكر من السبعينيات، اعتمدت بعض الدول الأوروبية قوانين حماية البيانات، بموجب الحق في الخصوصية الذي تكفله الاتفاقية الأوروبية لحماية حقوق الإنسان

والحريات الأساسية (1959). وكانت ولاية هيسن الألمانية أول من اعتمد هذا النوع من التشريعات .

وسرعان ما تبعتها السويد عام 1973 وجمهورية ألمانيا الاتحادية عام 1977، ثم فرنسا والنمسا والدنمارك والنرويج عام 1978، ويمكن تقديم هذه النصوص على أنها الجيل الأول من قوانين حماية البيانات([1]).

وأن كان يُنظَر إلى الإنترنت باعتبارها مساحة من الحرية النسبية ـ ليس فقط لأن مستخدميها قادرون على التواصل بشكل مجهول إلى حد ما، بل وأيضاً لأن هذا الفضاء أفلت من أي تنظيم من قِبَل الدولة.

وأن كنا تحدثنا عن "الفضاء السيبراني" لوصف هذا العالم الجديد لشبكات الكمبيوتر عبر الإنترنت التي أضيفت إليها أجهزة جديدة، مثل الهواتف الذكية والأجهزة اللوحية. ويغطي الفضاء السيبرانى الكوكب بأكمله، ويتجاهل الحدود الوطنية.

ومع ذلك، كما رأينا، تتعهد الدول بتنظيمه، كما هو الحال بالفعل بالنسبة للعالم المادي. وفي عام 1995، تم اعتماد اقتراح لتوجيه بشأن حماية البيانات الشخصية، يهدف إلى إزالة العقبات التي تعترض حرية حركتها داخل الاتحاد الأوروبي، من قبل البرلمان الأوروبي والمجلس (التوجيه 46/95)، ومن ثم يتم دمجها في قوانين الدول الأعضاء لتشكل ما يسمى بالجيل الثاني من قوانين حماية البيانات، إذا كانت إزالة الحواجز داخل السوق المشتركة هي الاختصاص التشريعي الرئيسي للاتحاد الأوروبي، فإن الحق في احترام الحياة الخاصة يؤخذ في الاعتبار بنفس طريقة حرية حركة البيانات الشخصية.

ومع ذلك، لم يكن من المتوقع حدوث مزيد من التطوير للتكنولوجيات الجديدة في التوجيه، حيث أن نقلها إلى قوانين الدول الأعضاء يمثل تباينات. وقد دفع ذلك المفوضية الأوروبية إلى استبدال التوجيه EC 46/1995/ باللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) في 25 مايو 2018 والتى عززت من خصوصية المواطن الاوروبي، وأسهمت في حماية بياناته الشخصية إلى جانب

---

[1] وكانت المادة الثامنة من الاتفاقية والتى تنص على الحق في احترام الحياة الخاصة والعائلية مهد القوانين التى تسعى الى حماية البيانات الشخصية باعتبارها حق للشخص ولذلك تقرر المادة أن :

1.لكل شخص الحق في احترام حياته الخاصة والعائلية وحرمة منزله ومراسلاته

2. .لا يجوز حصول تدخل من السلطة العامة في ممارسة هذا الحق، إلا بالقدر الذي ينص فيه القانون على هذا التدخل، والذي يشكل فيه هذا الأخير تدبيراً ضرورياً في اجملتمع الديمقراطي، للأمن الوطني أو السلامة العامة أو رفاهية البلد الاقتصادية أو الدفاع عن النظام أو منع الجرائم الجزائية أو حماية الصحة أو الأخلاق أو حماية حقوق الغير وحرياته اتفاقية حماية حقوق الإنسان في نطاق مجلس أوروبا روما في 4 نوفمبر 1950.

الترسيخ لفكرة السيادة الرقمية على بيانات الأفراد داخل الاتحاد الأوروبى من خلال ضمان مجموعة من الضوابط والحقوق، أهمها :

**الحق في الموافقة**: ويتمثل فى حق المواطن الأوروبي فى الموافقة الصريحة على السماح للشركات بتجميع بياناته الشخصية، وتوضيح سبب واضح لمعالجة هذه البيانات بعد تجميعها.

**والحق في الوصول إلى البيانات ونقلها**: أقرت اللائحة حق المواطن االأوروبي في الحصول على بياناته الشخصية ونقلها؛ وإعادة استخدامها في خدمات أخرى .والحق في إزالة البيانات: فيحق للمواطن الأوروبي طلب إزالة بياناته الشخصية لدى الجهات التي قامت بتجميعها، وذلك فيما يعرف بالحق النسيان الرقمى right to be forgotten ولذلك أجبرت المحكمة الأوروبية قبل تاريخ صدور اللائحة شركة Google على السماح لمواطني الاتحاد الأوروبي بإزالة جميع بياناتهم الشخصية استنادا إلى هذا الحق.

**الحق في المعرفة**: حيث تمنح اللائحة المواطن الأوروبي الحق في معرفة البيانات الشخصية التي يتم تخزينها عنه، وفيما سيتم استخدامها، إلى جانب الحق في تصحيح البيانات وتقييد وتحديد طريقة معالجة هذه البيانات والطريقة التي تتم بها معالجة بياناته الشخصية، وتلزم الجهات والشركات بالابلاغ في حال فقدان هذه البيانات أو سرقتها أو اختراقها.

ومن القوانين الرائدة فى التأصيل لفكرة السيادة الرقمية قانون Marco Civil Law of the Internet in Brazil الصادر عام 2014 واشترط هذا القانون على مقدمى خدمة الإنترنت واجب إلا يقدم المعلومات التى يجمعها سواء بشكل منفصل أو مرتبط بالبيانات الشخصية أو غيرها من المعلومات التي تسمح بتحديد هوية المستخدم أو المحطة، إلا بناءً على أمر قضائي، كما هو منصوص عليه في القسم الرابع من هذا الفصل، بما يتوافق مع ما هو المنصوص عليها في الفصل السابع.

كما لا يجوز إتاحة محتوى الاتصالات الخاصة إلا بأمر من المحكمة، في الحالات وبالطريقة التي يحددها القانون، وبما يتوافق مع البندين الثاني والثالث من المادة السابعه.

وفى ترسخيه لفكرة سيطرة الدولة على محتوها الرقمى نص على أن لا يمنع السلطات الإدارية من الوصول إلى البيانات المسجلة التي تحدد المؤهلات الشخصية والانتماء والعنوان، وفقًا لما ينص عليه القانون.

ويجب أن يتم إتخاذ تدابير وإجراءات الأمن والسرية بطريقة واضحة من قبل الشخص المسؤول عن تقديم الخدمات، وأن تستوفي المعايير المنصوص عليها في اللائحة، بما يتوافق مع حقوق سرية وأسرار العمل.

بينما نص فى المادة 11على أن أي عملية لجمع وتخزين والاحتفاظ ومعالجة البيانات الشخصية أو بيانات الاتصالات من قبل موفري الاتصال ومقدمي تطبيقات الإنترنت، يجب أن يحدث أحد هذه الأفعال على الأقل في الأراضي الوطنية، كما يجب

أن يكون احترام القانون البرازيلي إلزاميًا، بما في ذلك ما يتعلق بالحق في الخصوصية وحماية البيانات الشخصية وسرية الاتصالات الخاصة والسجلات، وينطبق هذا النص على البيانات المجمعة في الأراضي الوطنية، وعلى محتوى الاتصالات التي يوجد فيها أحد اطراف العلاقة على الأقل في البرازيل، ويجب على موفري الاتصال ومقدمي تطبيقات الإنترنت، تقديم على النحو المنصوص عليه في اللوائح، معلومات تسمح بالتحقق فيما يتعلق بامتثالها للتشريعات البرازيلية، فيما يتعلق بجمع البيانات وتخزينها والاحتفاظ بها ومعالجتها، وكذلك فيما يتعلق احترام الخصوصية وسرية الاتصالات([1]).

**قانون حماية البيانات لعام 2018** (DPA) هو القانون الأساسي لحكومة المملكة المتحدة، ويهتم هذا القانون بشأن معالجة البيانات الشخصية في المملكة المتحدة. والذي يتم تنفيذه جنبًا إلى جنب مع اللائحة العامة لحماية البيانات في المملكة المتحدة، إذ يُعد بمثابة إطار لحماية البيانات وينظم جميع الجوانب فى كيفية تحكم الشركات والمؤسسات والهيئات الحكومية في البيانات الشخصية ومعالجتها.

وينطبق هذا على جميع مراقبي البيانات حيث يتطلب قانون حماية البيانات من جميع مراقبي البيانات في المملكة المتحدة (الشركات والمؤسسات التي تتحكم في معالجة البيانات الشخصية تنفيذ التدابير الأمنية المناسبة لحماية البيانات الشخصية، والحفاظ عليها، وبشكل أكثر تحديدًا ينطبق هذا على الشركات التي تقوم عادة بمعالجة بيانات العملاء وسجلاتهم([2]).

**ومن القوانين التى ترسخ لفكرة السيادة الرقمية قانون تكنولوجيا المعلومات الصادر فى الهند Information Technology (**[3]**)Act 2000** ويُلزم الشركات التكنولوجية التي تمارس أعمالها في الهند، بما في ذلك الكيانات المسجلة في البلاد، وتلك التي تستعين بمصادر خارجية هناك، وتلك التي تحتفظ بالخوادم داخل حدود

---

**(1) Art 11.** In any operation of collection, storage, retention and treating of personal data or communications data by connection providers and internet applications providers where, at least, one of these acts takes place in the national territory, the Brazilian law must be mandatorily respected, including in regard the rights to privacy, to protection of personal data, and to secrecy of private communications and of logs. **LAW No. 12.965, APRIL 23RD 2014.**

(2) About International Telecommunication Union (ITU), ITU UN Agency website, retrieved from https://www. itu.int/en/about/Pages/default.aspx

(3) The Information Technology ACT, 2000 ACT NO. 21 OF 2000-India- retrieved from https://www. indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29

البلاد. أن يلتزموا بالقانون الهندى، ويغطي القانون جميع الأنشطة التي تنطوي على الوثائق الإلكترونية والتبادلات عبر الإنترنت([1]).

وتلتزم هذه الشركات والتى تقدم الخدمات الإلكترونية بأن يكون لديهم حضورًا فعليًا، ويعملون إلكترونيًا داخل حدود الدولة، فهم ملزمون بأحكام القانون ويتعين عليهم الاحتفاظ بسجلات معينة لفترة محددة داخل الحدود الوطنية([2]).

ويجب أن تكون هذه السجلات تحت تصرف وكالات إنفاذ القانون. ويعتبر عدم الامتثال لهذا الشرط جريمة يعاقب عليها بالسجن لمدة تصل إلى ثلاث سنوات أو/ وغرامة، ويجب على الشركات وموظفيها اتخاذ تدابير محددة أو التوقف عن ممارسة أنشطة محددة إذا اعتقدت السلطات أن مثل هذه الإجراءات ضرورية لضمان الامتثال لقانون تكنولوجيا المعلومات لعام 2000، وأى شخص يخالف هذا الامتثال يعتبر مذنبًا بارتكاب جريمة يعاقب عليها بالسجن لمدة تصل إلى ثلاث سنوات، وقد يُضطر هذا الشخص أيضًا إلى دفع غرامة تصل إلى 200 ألف روبيه([3]).

وتتمتع السلطات الحكومية في الهند بسلطة اعتراض أي معلومات يتم نقلها عبر موارد الكمبيوتر في ظل الظروف التالية: إذا كان من الضرورى القيام بذلك لصالح سيادة أو سلامة الهند، أو فى ذلك الاعتراض صالح أمن الدولة والحفاظ على العلاقات مع الدولة الأجنبية، أو تحقيق المصلحة للنظام العام فى الدولة.

وفى هذا النطاق نص الدستور المصرى على أن أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومى، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذى ينظمه القانون.

ويقرر القانون رقم 10 لسنة 2003 لتنظيم الاتصالات للسلطات المختصة في الدولة أن تخضع لإدارتها جميع خدمات وشبكات الاتصالات وأي مشغل أو مقدم خدمة وأن تستدعي العاملين لديه والقائمين على تشغيل وصيانة تلك الخدمات والشبكات وذلك في حالة حدوث كارثة طبيعية أو بيئية أو في الحالات التي تعلن فيها التعبئة العامة طبقا للقانون رقم 87 لسنة 1960 المشار إليه وأية حالات أخرى تتعلق بالأمن القومي.

---

(1) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person

(2) Chapter Ix 5 [Penalties, Compensation And Adjudication].

(3) **Art65** "Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both"

إضافة إلى ذلك هناك مجموعة من النصوص القانونية التى أصدرتها الدولة المصرية التى تواكب التشريعات الدولية فى الترسيخ لمبدأ سيادة الدولة الرقمية على بياناتها، والمعلومات التى يتم تدولها على شبكة الإنترنت، ومنها قانون 175 لسنة 2018 الخاص بمكافحة جرائم تقنية المعلومات، والذى وضع حماية للبنية التحتية الرقمية في الدولة، وجاء فى اللائحة التنفيذية لهذا القانون تحديد ماهية البنية التحتية التى تشكل فى مضمونها تطبيق لسيادة الدولة على بياناتها، وذلك بقولها أن **البنيـة التحتيـة المعلوماتية الحـرجة Critical Information Infrastructure** هى مجموعة أنظمة أو شبكات أو أصول معلوماتية أساسية يؤدى الكشف عن تفصيلاتها تعطيلها أو تغيير طريقة عملها بطريقة غير مشروعة، أو الدخول غير المصرح به عليها، أو الدخول أو الوصول بشكل غير قانونى للبيانات والمعلومات التى تحفظها أو تعالجها، أو يؤدى القيام بأى فعل غير مشروع آخر بها إلى التأثير على توافر خدمات الدولة ومرافقها الأساسية أو خسائر اقتصـادية أو اجتمـاعية كبـيرة على المستـوى الوطني.

ويعد من البنية التحتية المعلوماتية الحرجة على الأخص ما يستخدم في الطاقة الكهربائية، الغاز الطبيعى والبترول، الاتصالات، والجهات المـالية والبنوك، والصناعات المختلفة، والنقل والمواصلات والطيران المدنى، والتعليم والبحث العلمى، والبث الإذاعي والتليفزيوني، ومحطات مياه الشرب والصرف الصحى والموارد المـائية ، والصحة، الخدمات الحكومية وخدمات الإغاثة وخدمات الطوارئ، وغيرها من مرافق المعلومات والاتصالات التى قد تؤثر على الأمن القومى أو الاقتصاد القومى والمصلحة العامة وما في حكمها.

إضافة إلى أن القانون عمل على حماية المعلومات والبيانات عن طريق نظام التشفير ونص على أن يلتزم مقدمو خدمات تقنيات المعلومات باتخاذ الإجراءات التقنية والتنظيمية التالية تنفيذًا للبندين (2 و3) من الفقرة الأولى من المـادة رقم (2) من القانون ويقرر النص تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسى متماثل أو غير متماثل لا يقل في تأمينه عن Advanced Encryption Standard (ASE-128)([1])بمفتاح شفرة لا يقـل عن (128 بت)، مع مسئوليته بالحفاظ على سرية وأمان مفتاح التشفير .

---

[1] AES (معيار التشفير المتقدم) هو خوارزمية تشفير كتلي متماثل تقوم بتشفير البيانات في كتل مكونة من 128 بت باستخدام مفاتيح تشفير مكونة من 128 أو 192 أو 256 بت. ويعتبر هذا المعيار آمنًا ضد جميع الهجمات المعروفة ويتم اعتماده على نطاق واسع كمعيار لتشفير البيانات الإلكترونية. تم تأسيس AES بواسطة المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة في عام 2001. ومنذ ذلك الحين، أصبح خوارزمية مستخدمة على نطاق واسع للتشفير باستخدام المفتاح المتماثل.

وفى المحافظة على البنية التحتية الرقمية الخاصة بالدولة تقرر اللائحة التنفيذية للقانون أن يلتزم مقدمو خدمات تقنية المعلومات والاتصالات التى تمتلك أو تدير أو تشغل البنية التحتية المعلوماتية الحرجة المخاطبين بأحكام هذا القانون ، باتخاذ الإجراءات التقنية والتنظيمية التالية، إعداد سياسة أمن معلومات واعتمادها من الإدارة العليا للبنية التحتية المعلوماتية الحرجة وضمان مراجعتها كل عام لضمان استمرار ملائمة وكفاية وفاعلية تلك السياسة، على أن تتضمن تلك السياسة متطلبات الأجهزة والجهات الرقابية والتنظيمية المختصة بالبنية التحتية المعلوماتية الحرجة، والمتطلبات القانونية ، والمتطلبات الخاصة بالموارد البشرية .

ولتطبيق سيادة الدولة على معلوماتها الحرجة تقرر أن يضمن مقدمو الخدمة التأكد من الامتثال لما ورد بهذا القانون ولائحته والقرارات التنفيذية ذات الصلة من التزامات تقنية أو تنظيمية أضافة إلى تشفير البيانات والمعلومات بما يحافظ على سريتها، وعدم اختراقها باستخدام نظام تشفير قياسى متماثل أو غير متماثل لا يقل تأمينه عن Advanced Encryption Standard (AES-256) بمفتاح شفرة لا يقل عن (256 بت) يتم توليده باستخدام نظام عشوائى آمن.

هذا التنظيم القانون للسيادة الرقمية اصبح ضرورياً فى ظل التطورات التكنولوجية المتسارعة والتوسع الكبير فى استخدام الفضاء الرقمى، فهو يساعد على حماية البيانات والمعلومات ويمنع استغلالها بشكل غير مشروع، إضافة إلى أن هذا التنظيم يعزز الثقة فى التعاملات الرقمية ويساعد على وضع قواعد تحكم الأنشطة السيبرانية، ويمكن الدول من أن تحافظ على استقلالها وسيادتها على مواردها الرقمية والبنية التحتية التكنولوجية مما يمنع التدخلات الخارجية.

## المطلب الثالث

## دور القضاءين الدستورى والإدارى فى الترسيخ لفكرة سيادة الدولة الرقمية.

### 1) دور القضاء الدستورى فى تعزيز السيادة الرقمية.

إن تسارع التطور الرقمي فى أعقاب التطور الشامل للإنترنت، أدى على مدى العقد الماضي إلى التأثير على السلطة السيادية للدول، من خلال مضاعفة مصادر وأشكال المعيارية في الفضاء السيبرانى والاتصال بالشبكة العنكبوتية، فهى شبكة غير مادية وغير إقليمية وعابرة للحدود الوطنية بطبيعتها.

ولذلك تجد الدول نفسها الآن في منافسة مع كيانات أخرى، تنتج أيضًا معايير معيارية، أو جهات فاعلة اقتصادية خاصة، أو هيئات دولية، مما يفقدها في الواقع على أراضيها، سلطة احتكار وإعلان وتطبيق سيادة القانون، وبالتالي فإن تطور الإنترنت

يعني ضمنياً إعادة توزيع السلطات، فالبنية الهرمية التقليدية للنظام القانوني للدولة([1])، لم تعد كما كانت فى الماضى، ولهذا تقرر **المحكمة الدستورية الفيدرالية الألمانية** سياقها لمعالجة البيانات الحديثة، صرحت "بأنه يشمل الحق العام في حماية البيانات الشخصية بموجب المادة 2.1 بالاقتران بالمادة 1.1 من القانون الأساسي حماية الفرد من جمع البيانات الشخصية وتخزينها واستخدامها ومشاركتها بشكل غير محدود، ويضمن الحق الأساسي السلطة الممنوحة للفرد لاتخاذ قرار مبدئي بشأن الكشف عن بياناته الشخصية واستخدامها .

إضافة إلى أنه لا يجوز فرض قيود على هذا الحق في" تقرير المصير المعلوماتي" إلا إذا كانت هناك مصلحة عامة غالبة، وهذه المصلحة تتطلب أساسًا قانونيًا يجب أن يكون دستوريًا في حد ذاته، ومتوافقًا مع مبدأ الوضوح القانوني في ظل سيادة القانون. ويجب على المشرع أيضًا، مراعاة مبدأ التناسب، ويجب عليه أيضًا وضع الضمانات التنظيمية وإلاجرائية التى تحد من خطر انتهاك الحق العام في حماية البيانات الشخصية([2]) .

وفى هذا النطاق قرر **المجلس الدستورى الفرنسى** أنه "لضمان عدم إتاحة المحتوى الإباحي المنشور على الإنترنت للقاصرين، يجب على هيئة تنظيم الوسائط السمعية والبصرية والاتصالات الرقمية، من ناحية، أن تنشئ نظامًا مرجعيًا يتعلق بأنظمة التحقق من العمر، ليتم تنفيذها من قبل ناشري خدمات الاتصال العامة عبر

---

(1) Valentine Martin, La République Numérique En Débat Au Parlement : Le Projet De Commissariat À La Souveraineté Numérique, Les Nouveaux Cahiers Du Conseil Constitutionnel - N° 57, Octobre 2017

(2) In the context of modern data processing, the general right of personality under Article 2.1 in conjunction with Article 1.1 of the Basic Law encompasses the protection of the individual against unlimited collection, storage, use and sharing of personal data. The fundamental right guarantees the authority conferred on the individual to, in principle, decide themselves on the disclosure and use of their personal data. Limitations of this right to "informational self-determination" are only permissible if there is an overriding public interest. They require a statutory basis that must be constitutional itself and comply with the principle of legal clarity under the rule of law. The legislator must furthermore observe the principle of proportionality. It must also put in place organisational and procedural safeguards that counter the risk of violating the general right of personality

الإنترنت، ومقدمي خدمات منصات مشاركة الفيديو، ومن ناحية أخرى، قد يتطلب منهم إجراء عمليات تدقيق لهذه الأنظمة([1]).

إلي جانب ذلك جعلت **المحكمة الدستورية الالمانية** من اختصاصها الحفاظ على سيادة الدولة من أى اخطار أو هجمات سيبرانية فتقرر" أنها تمتع المحكمة الدستورية الفيدرالية بسلطة قضائية لفحص ما إذا كانت القواعد المطعون فيها متوافقة مع الحقوق الأساسية المنصوص عليها في القانون الأساسي، حتى لو كانت الأحكام المطعون فيها تشير إلى أحكام حماية البيانات في القواعد القانونية للاتحاد الأوروبي، وبذلك لا تنطبق الإجراءات القانونية المتعلقة بحماية البيانات الخاصة بالاتحاد الأوروبي على صلاحيات جهاز المخابرات الفيدرالية فيما يتعلق باستخبارات الاتصالات الاستراتيجية المحلية والأجنبية وفقًا للمادة 4 الفقرة 2 الجملة 3 .TEU ووفقاً لهذا، فإن الأمن القومي على وجه الخصوص يظل مسؤولية الدول الأعضاء منفردة، وهذا ما يجعل فكرة السيادة الرقمية لدول الأعضاء فى الاتحاد الأوروبى أمرًا ضروريًا يجب النظر إليه باعتباره أداه لحماية الأمن والمصالح الوطنية ووسيلة لتعزيز الثقة وحماية الحقوق الخاصة بالدول فى العصر الرقمى.

ونجد فى حكم **محكمة العدل التابعة للاتحاد الأوروبي** السيادة الرقمية تتوافق بالفعل مع هدف الحفاظ على الأمن القومي، والذى يتوافق بدوره مع الاهتمام الأساسي المتمثل في حماية الوظائف الأساسية للدولة، والمصالح الأساسية للمجتمع.

ويشمل ذلك منع وقمع الأنشطة، التي من المحتمل أن تؤدي إلى زعزعة استقرار الهياكل الداعمة لبلد ما بشكل خطير في المجالات الدستورية أو السياسية أو الاقتصادية أو الاجتماعية، وعلى وجه الخصوص، تهديد المجتمع أو السكان أو الدولة بشكل مباشر، ولا سيما الأنشطة الإرهابية فى الفضاء السيبرانى([2]).

---

(1) pour garantir que les contenus pornographiques mis en ligne ne soient pas accessibles aux mineurs, l'Autorité de régulation de la communication audiovisuelle et numérique, d'une part, établit un référentiel relatif aux systèmes de vérification de l'âge devant être mis en œuvre par les éditeurs de service de communication au public en ligne et les fournisseurs de service de plateforme de partage de vidéos et, d'autre part, peut exiger de ceux-ci qu'ils fassent réaliser des audits de ces systèmes pour s'assurer de leur conformité à ce référentiel. Décision n° 2024-866 DC du 17 mai 2024, Loi visant à sécuriser et à réguler l'espace numérique.
https://www.conseil-constitutionnel.fr/decision/2024/2024866DC.htm

(2) **Vgl. Eugh**, Urteile vom 6. Oktober 2020, La Quadrature du Net u.a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 135 und Privacy International, C-623/17, EU:C:2020:790, Rn. 74; Urteil vom 5. April 2022, Commissioner of An Garda Síochána, C-140/20, EU:C:2022:258, Rn. 61; Urteil vom 20. September 2022, SpaceNet AG u.a., C-793/19 und C-794/19,

وتقرر **المحكمة الدستورية الألمانية** فى ترسيخها لتطبيق مبدأ السيادة الرقمية فى ظل التهديدات السيبرانية الحالية "إن احتمالات المخاطرة بالهجمات السيبرانية الدولية مرتفعة للغاية، وذلك في سياق التحول الرقمي للمجتمع والاقتصاد والإدارة والسياسة، وتعتمد جميع مجالات الحياة تقريبًا بشكل متزايد على بنية تحتية رقمية فعالة وأمنها، يتزايد باستمرار الأهمية المركزية لأنظمة تكنولوجيا المعلومات الآمنة والفعالة لتحقيق حرية الحقوق الأساسية([1])، كما أن الهيئات الدستورية وغيرها من المؤسسات الضرورية للحياة الدستورية تعتمد بشكل متزايد على استخدام أنظمة تكنولوجيا المعلومات من أجل القيام بمهامها.

وإن تحويل العمليات التناظرية سابقًا إلى عمليات رقمية، والاستخدام المتنقل والمتزايد لأنظمة تكنولوجيا المعلومات يزيد من الاعتماد عليها، بما في ذلك الجهات الفاعلة الحكومية([2])، مما يجعل قدرة الدولة على بسط سيطرتها عليها أمر ضرورياً ، بالإضافة إلى ذلك، فقد زادت التهديدات من الخارج بشكل كبير بسبب مواصلة تطوير الاتصالات الدولية والتكامل العام الوثيق عبر الحدود لظروف المعيشة بشكل عام أصبحت قدرات الجهات الفاعلة التي تنطلق منها التهديدات السيبرانية الآن كبيرة وتتطور باستمرار([3]).

وتقرر أن على هذه الخلفية، فإن التهديدات السيبرانية الدولية الواردة في القانون في المادة 5 فقرة 1 جملة 3 رقم 8 ز 10 تتعلق بمصالح مشتركة رفيعة المستوى، والتي قد يؤدي انتهاكها إلى إلحاق ضرر جسيم بالسلام الخارجي والداخلي والمصالح القانونية للدولة والأفراد([4]).

وتقرر المحكمة فى تعزيزها لسيادتها الرقمية أن الهجمات السيبرانية الدولية تستهدف البنى التحتية الرقمية الحيوية أو أنظمة تكنولوجيا المعلومات ذات الأهمية المماثلة وتؤدى إلى زعزعة استقرار المجتمع ويمكن أن تشكل تهديدًا للنظام الدستوري ووجود وأمن الحكومات الفيدرالية أو حكومات الولايات بالإضافة إلى التأثير على حياة الافراد، وقد تتمكن الجهات المعادية الحكومية وغير الحكومية من تعطيل البنية التحتية

---

EU:C:2022:702, Rn. 92; Urteil vom 23. März 2023, Generalstaatsanwaltschaft Bamberg, C-365/21, EU:C:2023:236, Rn. 55).

(1) Vgl. BVerfGE 120, 274 <303 ff.>; 158, 170 <185 Rn. 33> – IT-Sicherheitslücken.

(2) vgl BVerfGE 158, 170 <185 Rn. 33.

(3) Vgl. EGMR <GK>, Big Brother Watch et al. v. the United Kingdom, Urteil vom 25. Mai 2021, Nr. 58170/13 u.a., Rn. 323; ENISA, Threat Landscape 2020, S. 8).

(4) Vgl. BVerfGE 100, 313 <373>; 154, 152 <248 f. Rn. 163.

الرقمية والأداء السليم للعمليات الديمقراطية وبالتالي تهديد الأمن القومي([1]). ويمكن أن يصل خطر الهجمات السيبرانية الدولية في نهاية المطاف إلى مستوى مماثل لخطر الهجوم المسلح على جمهورية ألمانيا الاتحادية، والذي تم الاعتراف به منذ البداية كسبب مشروع للمراقبة الاستراتيجية للاتصالات السلكية واللاسلكية في المادة 5 الفقرة 1 الجملة 3 رقم 3. 1 ز 10، ففي المجتمع المتحول رقميًا، يمكن أن يكون للهجمات السيبرانية المستهدفة والشاملة على البنية التحتية لتكنولوجيا المعلومات في المجالات الأساسية والحيوية (مثل إمدادات المياه والطاقة وكذلك أنظمة النقل والرعاية الصحية) تأثير هجوم مسلح. يمكن لكل من الهجمات السيبرانية الدولية والهجمات المسلحة أن تشكك في رفاهية السكان، والنظام الديمقراطي الليبرالي، وحتى وجود الدولة([2]).

وفى هذا الإطار تقرر **المحكمة الدستورية العليا المصرية** أن الدستور هو القانون الأساسى الأعلى الذى يرسى القواعد والأصول التى يقوم عليها نظام الحكم، ويحدد السلطات العامة، ويرسم لها وظائفها، ويضع الحدود والقيود الضابطة لنشاطها، ويقرر الحريات والحقوق العامة، ويرتب الضمانات الأساسية لحمايتها. ومن ثم، فقد تميز الدستور بطبيعة خاصة تضفى عليه السيادة والسمو بحسبانه كفيل الحريات وموئلها، وعماد الحريات الدستورية، وأساس نظامها، وحق لقواعده أن تستوى على القمة من البناء القانونى للدولة، وتتبوأ مقام الصدارة بين قواعد النظام العام باعتبارها أسمى القواعد الآمرة التى يتعين على الدولة التزامها فى تشريعاتها، وفى قضائها، وفيما تمارسه من سلطات تنفيذية، دون أية تفرقة أو تمييز فى مجال الالتزام بها، بين السلطات العامة الثلاث، التشريعية والتنفيذية والقضائية. وإذ كان خضوع الدولة بجميع سلطاتها لمبدأ سيادة الدستور أصلاً مقررًا، وحكمًا لازمًا، لكل نظام ديمقراطى سليم، فإنه يتعين على كل سلطة عامة، أيًّا كان شأنها، وأيًّا كانت وظيفتها، وطبيعة الاختصاصات المسندة إليها، أن تنزل على قواعد الدستور ومبادئه، وأن تلتزم حدوده وقيوده([3]).

وهذا يستدل منه على أن أمن الفضاء السيبرانى الذى يعد مجال تطبيق سيادة الدولة الرقمية ونجده ظاهره فى نص المادة 31 من الدستور المصرى والذى جعل أمن

---

(1) Vgl. EGMR <GK>, Big Brother Watch et al. v. the United Kingdom, Urteil vom 25. Mai 2021, Nr. 58170/13 u.a., Rn. 323

(2) In der digital transformierten Gesellschaft können gezielte und umfassende Cyberangriffe auf die IT-Infrastruktur elementarer und überlebenswichtiger Bereiche (etwa die Versorgung mit Wasser und Energie sowie das Transport- und Gesundheitswesen) wie ein bewaffneter Angriff wirken. Sowohl internationale Cyberangriffe als auch bewaffnete Angriffe können das Wohlergehen der Bevölkerung, die freiheitlich-demokratische Ordnung und sogar die Existenz des Staates in Frage stellen

([3]) حكم المحكمة الدستورية العليا: فى القضية رقم 18 لسنة 9 قضائية.

هذا الفضاء جزء أساسي من منظومة الأمن القومى وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه( [1] ).

وفى نطاق التوازن بين حرية الرأى والتعبير واعتبارها حرية ليست مطلقة من كل قيد تقرر المحكمة الدستورية العليا بأن حرية الرأى لا يقتصر أثرها على صاحب الرأى وحدة، بل يتعداه إلى غيره وإلي المجتمع، ومن ثم لم يطلق الدستور هذه الحرية، وإنما أباح تنظيمها بوضع القواعد والضوابط التى تبين كيفية ممارسة الحرية بما يكفل صونها فى إطارها المشروع دون أن تجاوزه إلى الأضرار بالغير والمجتمع( [2] ).

### 2) القضاء الإدارى ودوره فى ترسيخ السيادة الرقمية.

يلعب القضاء الإداري دورًا محوريًا في ترسيخ مفهوم السيادة الرقمية من خلال إصدار أحكام تضمن حماية الحقوق الرقمية وتنظيم استخدام التكنولوجيا والبيانات.

ويُعد القضاء الإدارى قضاء التوازن العادل بين سلطة الدولة فى بسط رقابتها القضائية وتطبيق قوانينها الداخلية _ المعبر عن سيادتها_ وبين الحرية المتمثلة فى حق الأفراد فى الوصول إلى الإنترنت باعتبارها اصبح اليوم من الحقوق الدستورية المعترف بها، إلى جانب ذلك فالقضاء الإدارى يوازن بين المصلحة العامة التى ترمى إليها الدولة من خلال إدارتها للمرافق الخاصة بها وبين المصلحة الخاصة بالأفراد المتمثلة فى ضمان حقوقهم وحرياتهم، وعليه نجد محكمة القضاء الإدارى تقرر " أن هناك ضوابط عند استعمال الأفراد لحقوقهم .... أولاً: مراعاة اعتبارات المصلحة العامة وحماية المجتمع وتقاليده دون أن يتخذ معيار المصلحة العامة ستاراً للعصف بالحقوق والحريات( [3]) وفى تطبيق مبدأ السيادة الرقمية الخاصة بالدولة على الفضاء السيبرانى يقرر **مجلس الدولة الفرنسى فى قضية "Network Data French"** في مدى توافق جمع وتخزين بيانات الاتصالات الإلكترونية مع حقوق الخصوصية وحماية البيانات الشخصية. إذ ينص على أن" فى حالة تفسير أحكام التوجيه الصادره فى 8 يونيو 2000 وكذلك المواد 6،7،8،11 من ميثاق الحقوق الأساسية للاتحاد الأوروبى، والتى تسمح لأى دولة بوضع لوائح وطنية تفرض على الأشخاص الذين يتمثل نشاطهم فى توفير الوصول إلى خدمات الإنترنت للجمهور، سواء كانوا اشخاص طبيعين أو اعتباريين التزام بالاحتفاظ بالبيانات التى من المحتمل أن تسمح بتحديد هوية الأشخاص أذا كان ذلك يحقق المصلحة العامة للدولة ويحمى الأمن القومى"( [4]) ،

---

(1) المادة 31 من الدستور المصرى الصادر 2014.

(2) حكم المحكمة الدستورية العليا فى القضية رقم 14 لسنة 7 قضائية دستورية بجلسة 7/ 5/ 1988 ج 4 ، ص 98.

(3) حكم محكمة القضاء الإدارى فى الدعوى رقم 1593 لسنة 5 قضاء إدارى بجلسة 7/ 11/ 1951.

(4) Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des

وأصدر المجلس حكمًا يوازن بين متطلبات الأمن القومي وحقوق الأفراد في الخصوصية، مؤكدًا على ضرورة أن تكون أي تدابير لجمع البيانات متناسبة ومحددة الأهداف( [1]).

**ومحكمة القضاء الإدارى** فى مصر عند نظرها في مسألة حجب موقع "يوتيوب"، فى إطار التكريس لمفهوم سيادة الدولة على الفضاء السيبرانى المتمثل فى الموقع المذكور تقرر" أن ما يعرض على هذه المواقع يعد من أبرز صور الاخلال بالمصالح العليا للدولة، والأمن القومى الاجتماعى، ومن ثم كان لزاماً على الجهة الإدارية اتخاذ كافة الوسائل اللازمة لحجب هذه المواقع عن المواطن المصرى، ومن ثم يضحى جلياً ثبوت المخالفة فى حق موقع اليوتيوب، وكذلك جميع الروابط الالكترونية على الإنترنت التى تعرضه"( [2]).

وفى سبيلها إلى حماية القيم الدينية والمجتمعية؛ رأت المحكمة أن عرض محتوى مسيء للأديان يتعارض مع القيم الدينية والأخلاقية للمجتمع المصرى، قررت المحكمة " وقد استقر قضاء هذه المحكمة على أنها وهى تنتصر للمبادئ والقيم الاخلاقية التى يقوم عليها الإعلام المرئ والمسموع والمقروء فى نطاق الانحياز لحرية الرأى والتعبير المسئولة، فإنها تهيب بالجهة الإدارية الوقوف عند مسئولياتها وتنوه إلى أن مسئوليتها جد خطيرة فى الا تقهر رأياً أو فكراً ..... إلا إنه فى ذات الوقت يقع على كاهلها حماية القيم والاخلاق وحماية المعتقدات الدينية والأسرة المصرية( [3]).

و أكدت أن الدولة مسؤولة عن حماية المقدسات الدينية وضمان عدم المساس بها، وقررت تغليب المصلحة العامة على المصلحة الخاصة واعتبرت أن حجب "يوتيوب" لفترة مؤقتة هو إجراء ضروري لحماية المصلحة العامة، حتى لو تأثرت

---

droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un Etat d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale

([1]) Conseil d'État, Assemblée, 21/04/2021, 393099, Publié au recueil Lebon.

[(2)] حكم محكمة القضاء الإدارى فى الدعوى رقم 60693 لسنة 66 ق ، بجلسة 2013/2/9

[(3)] حكم محكمة القضاء الإدارى فى الدعوى رقم 60693 لسنة 66 ق ، بجلسة 2013/2/9

بعض الحريات مثل حرية التعبير أو الأعمال المرتبطة بالمنصة، إلى جانب الالتزام بمبادئ الأمن القومي ، أشارت المحكمة إلى أن أي محتوى يهدد الأمن القومي، أو يُثير الفتنة الطائفية، يجب أن يُواجه بإجراءات حاسمة من الدولة، بما في ذلك الحجب المؤقت للمواقع.

المحكمة ركزت على التوفيق بين صيانة الأمن القومي والقيم المجتمعية وبين الحقوق الدستورية للمواطنين، وأكدت أن الحجب جاء كإجراء استثنائي ومؤقت لحماية المصلحة العامة.

وفى ذات النطاق أكدت **المحكمة الإدارية العليا** على ذات المعانى فى حكمها الصادر 2018 و رسخت المحكمة فكرة السيادة الرقمية وأن كانت لم تتطرق إلى النص صراحة ولكنها تناولت حق الأجهزة الحكومية والجهاز القومى لتنظيم الاتصالات فى حجب المواقع اذا كانت هناك مساس بالأمن القومى أو المصالح العليا للدولة وذلك بما تملكه الأجهزة من سلطة فى مجال الضبط الإدارى لحماية النظام العام بعناصره الثلاث.

وتقرر" إن قضاء هذه المحكمة قد جرى على أن الدستور المصرى مسايرًا في ذلك الاتفاقيات الدولية المقررة لحقوق الإنسان قد كفل حرية التعبير بمدلوله العام ، وفي مجالاته المختلفة السياسية والاقتصادية والاجتماعية وبجميع وسائل التعبير وضماناً من الدستور الحرية التعبير والتمكين من عرضها ونشرها بأى وسيلة، وعلى ذلك فإن هذه الحرية لا تنفصل عن الديمقراطية، وأن ما توخاه الدستور من خلال ضمان حرية التعبير هو أن يكون التماس الآراء والأفكار وتلقيها عن الغير ونقلها إليه غير مقيدة بالحدود الإقليمية على اختلافها، ولا تنحصر في مصادر بذواتها بل قصد أن تترامى إقامتها، وأن تتعدد مواردها وأدواتها معصومة من ثمة أغلال أو قيود إلا تلك التي تفرزها تقاليد المجتمع وقيمه وثوابته بحسبان أن الحريات والحقوق العامة التي كفلها الدستور ليست حريات وحقوق مطلقة وإنما هي مقيدة بالحفاظ على الطابع الأصيل لقيم المجتمع وثوابته وتقاليده والتراث التاريخي للشعب والحقائق العلمية والآداب العامة، وقد انتظم القانون رقم 10 لسنة 2003 بشأن تنظيم الاتصالات مبادئ وقواعد لتنظيم جميع أنواع الاتصالات، إلا ما استثنى بنص خاص، وناط بالجهاز القومى لتنظيم الاتصالات وبوزير الاتصالات وتكنولوجيا المعلومات تنظيم وسائل إرسال أو استقبال الرموز أو الإشارات أو الرسائل أو الكتابات أو الصور أو الأصوات، وذلك أيا كانت طبيعتها، كان الاتصال سلكياً أو لاسلكياً، وخدمة الاتصالات الدولية بين المستخدمين في مصر وبين الدول الأجنبية من خلال المعابر الدولية للاتصالات بما في ذلك الطيف الترددي الذي يمثل حيز الموجات التي يمكن استخدامها فى الاتصال اللاسلكي طبقاً لإصدارات الاتحاد الدولى، وضمان الاستخدام الأمثل لهذا الطيف مع مواكبة التقدم العلمى والفنى والتكنولوجي ووضع قواعد وشروط منح التراخيص الخاصة باستخدام الطيف، وإصدار هذه التراخيص وتجديدها وإلغائها

ومراقبة تنفيذها وذلك كله بما لا يخل بالمصلحة العليا للدولة والأمن القومي للبلاد، ولئن كانت التشريعات المصرية بما فيها قانون تنظيم الاتصالات لم تحدد الحالات التي تستدعى حجب المواقع الإلكترونية، إلا أن ذلك لا يخل بحق الأجهزة الحكومية والجهاز القومى لتنظيم الاتصالات في حجب بعض المواقع على الشبكة الدولية للانترنت حينما يكون هناك مساس بالأمن القومى أو المصالح العليا للدولة وذلك بما لتلك الأجهزة من سلطة في مجال الضبط الإدارى لحماية النظام العام بمفهومه المثلث، الأمن العام والصحة العامة والسكينة العامة للمواطنين تحت رقابة القضاء"([1]).

وبذلك يساهم القضاء الإدارى بفاعلية فى الترسيخ لفكرة السيادة الرقمية من خلال ضمان تطبيق القوانين وحماية الحقوق فى البئية الرقمية، والرقابة على إعمال الإدارة والتأكد من توافقها مع مبادئ المشروعية مما يرسخ سيادة القانون فى المجال الرقمى.

# الفصل الثانى

# تحديات السيادة الرقمية

في عصر الثورة الرقمية، أصبحت البيانات والمعلومات الرقمية من الأصول الأكثر قيمة، ومع ذلك، فإن السيطرة عليها تثير تحديات كبيرة، خاصة عندما تتجاوز الحدود الوطنية، هذا ما دفع الدول إلى تبني مفهوم السيادة الرقمية لتعزيز التحكم في مواردها الرقمية وتقليل الاعتماد على الكيانات الخارجية.

وأن كانت السيادة الرقمية (Digital Sovereignty) تشير إلى قدرة الدول أو الكيانات على التحكم في بياناتها الرقمية، وأنظمتها التقنية، وقوانينها المتعلقة بالفضاء السيبراني. إلا إن تطبيق هذه الفكرة تواجه تحديات متعددة؛ منها ما هو قانونى ومنها اقتصادى ومنها ما هو تقنى، إضافة إلى التوافق بين حرية الإنترنت التى تعد مبدأ من المبادئ التى تم التأصيل لها فى المواثيق الدولية والدساتير الوطنية وبين تطبيق سيادة الدولة الرقمية التى تُعد خطوة حيوية لتحقيق استقلالية الدول في الفضاء الرقمي، هذه التحديات نناقشها فى مطلبين الأول منهما يتناول التحديات القانونية

---

[1] حكم المحكمة الإدارية العليا فى الطعنين رقم 10464 و 10558 لسنة 59 قضائية عليا بالجلسة المنعقدة يوم السبت الموافق 2018/5/26.

والاقتصادية والتى تواجه فكرة السيادة الرقمية، بينما المطلب الثانى نناقش تحقيق التوافق بين مبدأ حرية الإنترنت كمبدأ دستورى وتطبيق الدولة لسيادتها الرقمية ، هذا فى المبحث الأول، ثم نتطرق إلى نماذج من الأنظمة المقارنة التى سعت إلى تحقيق السيادة الرقمية، وأخيراً مساعى الدولة المصرية فى تحقيق الاستقلال الرقمى وفرض السيادة المصرية على البيانات والمعلومات الخاصة بها وذلك فى المبحث الثانى، على النحو التالى:

المبحث الأول: التحديات التى تواجه تطبيق السيادة الرقمية.

المبحث الثانى: جهود الدول نحو تحقيق السيادة الرقمية.

# المبحث الأول

## التحديات التى تواجه تطبيق السيادة الرقمية.

فى ظل العولمة الرقمية تواجه الدول تحديات كبيرة تنعلق بتطبيق سيادتها الرقمية فى الفضائ السيبرانى، هذه التحديات نناقشها فى مطلبين الأول منهما يتناول التحديات القانونية والاقتصادية التى تواجه فكرة السيادة الرقمية، بينما المطلب الثانى نناقش تحقيق التوافق بين مبدأ حرية الإنترنت كمبدأ دستورى وتطبيق الدولة لسيادتها الرقمية.

### المطلب الأول

### التحديات القانونية والاقتصادية التى تواجه فكرة السيادة الرقمية

السيادة الرقمية مفهوم حديث نسبياً وغير محدد بشكل كامل، ما يتركه عرضة لتفسيرات متباينة تؤدي إلى تحديات قانونية واقتصادية فى تطبيق هذا المفهوم هذه التحديات هى:

**اولاً: التحديات القانونية.**

يُعد الإنترنت فضاء عالمي، يتجاوز الحدود الوطنية، ولذلك تختلف القوانين المتعلقة بالبيانات وحماية الخصوصية من بلد إلى آخر (مثل الفرق بين اللائحة العامة لحماية البيانات في الاتحاد الأوروبي GDPR والقوانين الأمريكية)، هذا التعارض يخلق صعوبات في فرض السيادة الرقمية على المستوى الدولي وعلى المستوى الوطنى.

ولهذا فالسيادة الرقمية تُواجه تحديات تتعلق بتضارب القوانين الدولية والمحلية بشأن تدفق البيانات وحوكمتها، ففي ظل العولمة الرقميةDigital Globalization اصبحت شبكة الويب العالمية توفر الروابط التى تربط الاقتصاد العالمى ببعضه

البعض، ولتأمل هذه الحقيقة نجد حقيقة مفادها أن نحو 50% من الخدمات المتداولة فى العالم أصبحت رقمية بالفعل، إضافة إلى أن 12% من تجارة السلع تتم عبر التجارة الإلكترونية الدولية([1])، ولهذا غالبًا ما تكون التشريعات الوطنية غير متوافقة مع الاتفاقيات الدولية المتعلقة بحرية تدفق البيانات.

ونجد أن تأثير ذلك: يخلق نوع من التضارب ويؤدى إلى فجوة تشريعية تؤثر على الشركات المحلية والدولية وتضعف الجهود المبذولة لتحقيق سيطرة كاملة على البيانات.

هذا التضارب نجده واضح فى القوانين الأمريكية وقوانين الاتحاد الأوروبى اللذان تناول حماية البيانات؛ فنجد فمثلاً قانون السحابة الأمريكية Cloud Act يتيح إمكانية وصول السلطات الأمريكية إلى البيانات الشخصية المخزنة في مراكز البيانات في أوروبا وأجزاء أخرى من العالم دون موافقة مسبقة، فقانون الحوسبة السحابية الأمريكي، المعروف رسميًا باسم "قانون توضيح الاستخدام القانوني للبيانات في الخارج"، هو قانون صدر في الولايات المتحدة في عام2018 ([2]).

ويثير قانون الحوسبة السحابية الأمريكي مخاوف كبيرة فيما يتعلق بحماية البيانات والخصوصية في أوروبا ودول العالم التى تعتمد على التكنولوجيا الامريكية . نظرًا لأنه يمنح السلطات الأمريكية حق الوصول غير المقيد إلى البيانات المخزنة خارج الولايات المتحدة، فقد تخضع الشركات والمنظمات الأوروبية والشركات العاملة فى الدول الأخرى التي تستخدم خدمات الحوسبة السحابية أو حلول البرامج الأمريكية للمراقبة من قبل السلطات الأمريكية دون علمها. ولا يوجد التزام من جانب الولايات المتحدة بإبلاغ الأطراف المتضررة.

هذا وتواجه الشركات والسلطات الأوروبية تحدي الامتثال لقواعد حماية البيانات في الاتحاد الأوروبي، وخاصة اللائحة العامة لحماية البيانات GDPR، وضمان الحماية الكاملة للبيانات وسيادة البيانات أثناء استخدام البرامج والخدمات السحابية الأمريكية. ولهذا يصبح الامتثال لمعايير حماية البيانات أمرًا صعبًا بمجرد ملامستها للحوسبة السحابية الأمريكية بأي شكل من الأشكال.

ولذلك هناك قاعدة هامة جدة فى هذا الشأن وهى: أن تخضع البيانات المخزنة التي تتم معالجتها في أوروبا للوائح الاتحاد الأوروبي، وبالتالي اللائحة العامة لحماية البيانات هى الواجبة التطبيق.

---

**(1) Daniel Castro and Alan McQuinn**: Cross-border data flows enable growth in all industries, Information Technology and Innovation Foundation, February 2015. Referred to the McKinsey Global Institute (MGI), Digital Globalization: The New Era Of Global Flows, P33.

(2) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including ter rorism.

ولا يوجد اتفاق بين الاتحاد الأوروبي والولايات المتحدة يتناول قانون الحوسبة السحابية على وجه التحديد، وبالتالي، فإن مجرد نقل البيانات المخزنة في الاتحاد الأوروبي إلى الخارج يشكل تلقائيًا انتهاكًا للائحة العامة لحماية البيانات. ولا يمكن تجنب ذلك إلا باستخدام برامج أوروبية تتوافق مع اللائحة العامة لحماية البيانات الأوروبية.

ومن الامثلة على التضارب بين القواعد القانونية التى تسعى كل دولة أن تطبيقها على سيادتها الرقمية فى حفظها للبيانات المخزنة على السحابة الخاصة بها نجد هناك تحديات يفرضها قانون الحوسبة السحابية الأميركي على لوائح حماية البيانات الأوروبية هو الاتفاق الإطاري بين الإدارة الفيدرالية الألمانية وشركات مثل Oracle &Microsoft. وتسمح هذه الاتفاقيات لهذه الشركات بتقديم خدمات الحوسبة السحابية وحلول البرمجيات للحكومة الألمانية([1]).

وقد أثار هذا الاتفاق مخاوف بشأن حماية البيانات والقدرة على السيطرة على البيانات المتداولة فى الحدود الوطنية، حيث قد تتمكن السلطات الأميركية من الوصول إلى البيانات التي تخص المواطنين والسلطات الألمانية.

هذا ونجد أن فرض القوانين الوطنية على البيانات المتعلقة بالدولة أو مواطنيها يواجه العديد من التحديات مثل الاتفاقيات الدولية التى تنظم الفضاء السيبرانى منها الاتفاقية الدولية لمكافحة الجريمة الإلكترونية" بودابست" التى تضع إطار قانونى موحد للتعامل مع الجرائم السيبرانية ولكن هذه الإتفاقية لم توقع عليها العديد من الدول

---

([1]) The new sovereign cloud region operates under a comprehensive set of policies and governance that further enhance OCI's existing internal capabilities for data residency, security, privacy, and compliance. These policies include a framework for data and operational sovereignty, including how OCI stores and manages access to data, and how data access from entities outside the EU are handled. The Oracle EU Sovereign Cloud data centers are located in the EU (Frankfurt, Germany and Madrid, Spain), and they are owned and operated by separate Oracle-owned EU legal entities incorporated within the EU, with operations and customer support restricted to EU-based personnel. Oracle EU Sovereign Cloud builds on Oracle Cloud's existing compliance programs that enable customers to demonstrate adherence to regional and industry regulations. It also aligns with EU monitoring regulations, and guidance that limits data transfers out of the EU (such as Court of Justice for EU Schrems II Ruling and European Data Protection Board), **Austin,** Press Release, Oracle Addresses European Data Privacy and Sovereignty Requirements with New EU Sovereign Cloud, Jun 2023,https://www.oracle.com/news/announcement/oracleaddresseseuropean-data-privacy-and-sovereignty-requirements-with-neweusovereigncloud2023-06-20/

مثل الصين وروسيا، مما يعرقل تطبيقها على المستوى الدولى، إضافة إلى أن الجرائم السيبرانية تتطور بسرعة تفوق قدرة الاتفاقية على التكيف معها، مما يجعل بعض بنودها غير كافية للتعامل مع الجرائم الحديثة مثل الجرائم المرتبطة بالذكاء الاصطناعى والعملات المشفرة.

ومما يدلل على التضارب الواضح هو ما اعلن عنه ممثل روسيا بأن هناك بعض البلدان التى تسعى إلى فرض قواعدهم فى الفضاء المعلوماتى على العالم اجمع، بناء على تكنولوجيتهم ومن خلال انجازتهم فى إشارة إلى الولايات المتحدة الامريكية([1]).

فالطبيعة العالمية والعابرة للحدود للفضاء السيبرانى والتى تقوم على أن هذا الفضاء نوع من المنافع العامة العالمية جعل التنظيم القانونى لهذا الفضاء يواجه صعوبات متعددة، فممارسة الدولة ولاياتها القضائية على الفضاء السيبرانى وتطبيق سيادتها الرقمية يؤدى فى كثير من الأحيان إلى التأثير على البنية التحتية السيبرانية لدول أخرى.

فالاختلافات فى الأنظمة القانونية الوطنية تجعل وضع إطار لتنظيم الفضاء السيبرانى يشوبه العديد من الصعوبات، إضافة إلى أن أى محاولة لتنظيم هذا الفضاء يتتطلب تعاون دولى وتبادل لعديد من البيانات بين الدول، مما يشكل مخاوف حول السيادة الوطنية وخصوصية البيانات المحلية([2]).

هذه التحديات التى تجعل فرض دولة ما سيادتها الرقمية على الفضاء السيبرانى الخاص بها، يتتطلب تعاون دولى وتنسيق بين الدول خاصة فى الجرائم العابرة للحدول إضافة إلى موافقة من دول أخرى لتطبيق ولاياتها القضائية، كل هذه الصعوبات القانونية يجعل من فرض السيادة الرقمية أمر يحتاج إلى المزيد من الدراسة لبحث التوافق القانونى للقواعد المراد تطبيقها على الفضاء السيبرانى.

**ثانياً: التحديات الاقتصادية والاستثمار فى البنية التحتية الرقمية.**

وعلى الصعيد الاقتصادي فإن الدولة تسعى لتأكيد سيادتها من خلال تأمين نظام سيبراني قوي يضمن أمان كافة المعاملات المالية والمصرفية التي باتت تعتمد على التكنولوجيا وحركة انتقال الأموال الإلكترونية بشكل كبير؛ حيث تُشجع الدول مواطنيها

---

([1]) certain countries that seek to impose their rules of the game in the information space on the whole world… Based on their technological achievements, they are trying to enforce the “rule of the gun” in the information space, **Vladimir Korovkin**: International Regulation In Cyber Space: Is Effective Mutual Understanding Possible?, January 2022 URL: https://sns-journal.ru/en/archive/

([2]) Position Paper, On the Application of International Law in Cyberspace , The position paper has been prepared by the German Federal Foreign Office and the German Federal Ministry of Defence in cooperation with the German Federal Ministry of the Interior, Building and Community, March 2021.

على التخلِّي عن استخدام الأموال نقدًا واعتماد المُعاملات الآلية بدلًا عنها؛ مما يتطلب توفير بنية تحتية كفؤة لتأمين هذه المعاملات المالية؛ وفي هذه الحالة يكون للدولة دور رئيسي في إدارة حركة انتقال الأموال والحد من الاقتصاد غير الرسمي وكافة أشكال التعاملات المالية الخارجة عن نطاق سيطرة الدولة وإدارتها؛ وفي هذا الإطار تسعى الدول بخطوات حثيثة لتطبيق سياسات الشمول المالي، ومن المؤكَّد أن مساعي الدولة لتأكيد سيادتها في الفضاء السيبراني يُرتِّب تطوُّرات قانونية جديدة تُمكن الدولة من تنظيم الفضاء الإلكتروني وممارسة سيادتها عليه، سواء في المعاملات الاقتصادية أو السياسية أو الاجتماعية، الأمر الذى يجعلها تواجه تحديات اقتصادية عديدة([1]).

وأن كانت السيادة الرقمية تعني قدرة الدول على التحكم في بياناتها الرقمية وأنظمتها التقنية، وحمايتها من النفوذ الأجنبي أو التبعية التكنولوجية. فمعا تطور الاقتصاد الرقمي، اصبحت الدول تواجه تحديات اقتصادية متعددة في تطبيق السيادة الرقمية، ومن التحديات الاقتصادية هذه ما يلى:

❖ **تكلفة تطوير البنية التحتية الرقمية.**

يشكل الاعتماد على التكنولوجيا الأجنبية تحدى كبير لدى الدول الراغبة فى تطبيق سيادتها على الفضاء الرقمى الخاص بها، إذ تعتمد العديد من الدول على الشركات الأجنبية لتوفير التكنولوجيا الأساسية مثل الخوادم والحوسبة السحابية.

هذا ما جعل الأمر يشكل ضغط على الدول التى تسعى إلى فرض سيطرتها على بياناتها الرقمية، ويؤدي إلى إنفاق كبير على استيراد الخدمات من الخارج مما يجعلها غير مستقلة بالكلية، إضافة إلى أن الاستثمار المحلي فى النبية التحتية الرقمية وإنشاء بنية تحتية وطنية يتطلب استثمارات ضخمة، مما قد يثقل كاهل الميزانيات الوطنية([2]).

❖ **نقص الكفاءات التكنولوجية المحلية.**

من التحديات التى تواجه الدول هى هجرة العقول؛ فتواجه الدول النامية تحديًا في الحفاظ على المواهب التقنية التي تهاجر إلى دول أكثر تقدمًا، إضافة إلى أن تكلفة التدريب وإعداد برامج تدريب الكوادر المحلية تستهلك موارد كبيرة وقد تكون طويلة الأمد.

❖ **التبعية الاقتصادية للشركات العالمية.**

تشكل هيمنة الشركات الكبرى تحدى لدى الدول التى تفكر فى الاستقلال الرقمى فالشركات مثلGoogle ، Amazon، Microsoftتسيطر على جزء كبير من الخدمات الرقمية والبنية التحتية السحابية، مما يقلل من قدرة الدول على التحكم في

---

([1]) رغدة البهي، الوكالة السيبرانية.. عوامل النشأة وأنماط الفواعل، مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 218، أكتوبر 2019، ص ص 15-20.

([2]) **Asif Raihan**: A review of the potential opportunities and challenges of the digital economy for sustainability, Innovation and Green Development, Volume 3, Issue 4, December 2024. P24.

بياناتها، إضافة إلى أن الشروط الاقتصادية التى تضعها هذه الشركات قد تكون مجحفة لكثير من الدول، نتيجة لهذا فالاعتماد على هذه الشركات قد يتطلب قبول شروط اقتصادية وتقنية غير ملائمة، مما يعنى أن فكرة تطبيق الدولة لسيادتها الرقمية يخضع فى جزء كبير منها لقواعد وشروط الشركات الكبرى

❖ **تأثيرات الحماية الاقتصادية.**

فالقيود على الاستثمار الأجنبي الخاص بالبنية التحتية الرقمية ومحاولة استقلال الدولة رقمياً، يشكل تحدى فى جذب الاستثمار الاجنبى، لذلك نجد أن فرض قيود على الشركات الأجنبية لحماية السيادة الرقمية قد يؤدي إلى تقليص الاستثمارات الأجنبية المباشرة، فتشديد الرقابة المحلية قد يحد من دخول الشركات التكنولوجيا للسوق المحلى، مما يعنى تقليل التنافسية فى الدول التى تعمل على هذا الاستقلال الرقمى، فحماية البيانات عبر الحدود: تتطلب فرض قيود على نقل البيانات بين الدول الأمر الذى يؤثر على الشركات المحلية التي تعتمد على التجارة الدولية، فتطبيق قوانين السيادة الرقمية قد تعيق عمل الشركات متعددة الجنسيات إلى جانب عدم التنسيق دولي حول قوانين السيادة الرقمية قد يؤدي إلى تعقيدات اقتصادية وتكاليف إضافية للشركات، فالدول التي تسعى لتطبيق سيادتها الرقمية بشكل صارم قد تواجه صعوبات في الاندماج مع الاقتصاد العالمي.

❖ **التكلفة العالية للأمن السيبراني.**

تطبيق السيادة الرقمية يعنى أن تكون الدول قادرة على صد الهجمات السيبرانية التى تتعلاض لها، الأمر الذى بدوره يجب على هذه الدول أن يكون لديها قدرة تكنولوجيا عالية من الأنظمة الأمنية التى تسطيع من خلالها صد مثل هذه الهجمات، ونتيجة لها يجب على الدول أن تعمل على ضخ استثمارات ضخمة لتطوير أنظمة أمان سيبراني قوية لحماية بياناتها من التهديدات، وأن تعمل على التحديثات المستمرة لأنظمة الأمان لديها الأمر الذى قد يكون مكلف جدًا على المدى الطويل.

نتيجة لهذا يعتبر تطبيق السيادة الرقمية ضرورة استراتيجية للحفاظ على أمن الدول واستقلالها التقني، لكنها تأتي بتحديات اقتصادية كبيرة تتطلب حلولاً مبتكرة واستثمارات مستدامة.

## المطلب الثانى

## تحقيق التوافق بين مبدأ حرية الإنترنت كمبدأ دستورى وتطبيق الدولة لسيادتها الرقمية.

وأن كانت تُشير حرية الإنترنت إلى حق الأفراد في الوصول إلى المعلومات وتبادلها بحرية عبر الشبكات الرقمية، وتُعد هذه الحرية أحد حقوق الإنسان الأساسية

المضمونة في المواثيق الدولية مثل الإعلان العالمي لحقوق الإنسان([1])، وتعد هذه الحرية ركيزة أساسية في المجتمعات الحديثة، حيث تسهم في تعزيز حرية التعبير والتواصل ([2]).

بل إن الأمم المتحدة أعلنت في تقرير لها بأن الوصول للإنترنت يعتبر حقاً من حقوق الإنسان وقطع هذه الخدمة عن المشتركين يعتبر بمثابة انتهاك للقانون الدولي لحقوق الإنسان([3]).

ونص قرار للمحكمة العليا في كوستاريكا صدر في الثلاثين من يوليو عام 2010 ما يلي« دون الخوف من المراوغة، يمكن أن نقول إن هذه التقنيات _ تقنيات المعلومات والاتصالات_ قد أثرت على طريقة تواصل البشر، حيث سهلت الاتصال بين البشر والمؤسسات في مختلف أرجاء العالم، كما حدت من قيود المسافة والزمن. وفي هذا الوقت، أصبح الوصول إلى هذه التقنيات أداة أساسية لتسهيل ممارسة الحقوق الأساسية والمشاركة الديمقراطية (الديمقراطية عبر الإنترنت) وسيطرة المواطن والتعليم وحرية التفكير والتعبير والوصول إلى المعلومات والخدمات العامة المتاحة عبر الإنترنت والحق في التواصل مع الحكومة إلكترونيًا والشفافية الإدارية وغير ذلك.

---

([1]) Art 19 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers", Universal Declaration of Human Rights.

([2]) N. Lucchi, "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011..

([3]) "any restriction to the right to freedom of expression must meet the strict criteria under international human rights law. A restriction on the right of individuals to express themselves through the Internet can take various forms, from technical measures to prevent access to certain content, such as blocking and filtering, to inadequate guarantees of the right to privacy and protection of personal data, which inhibit the dissemination of opinions and information. The Special Rapporteur is of the view that the arbitrary use of criminal law to sanction legitimate expression constitutes one of the gravest forms of restriction to the right, as it not only creates a “chilling effect”, but also leads to other human rights violations, such as arbitrary detention and torture and other forms of cruel, inhuman or degrading treatment or punishment"General Assembly , Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council Seventeenth session, 16 May 2011

ويشتمل هذا على الحق الأساسي في الوصول إلى هذه التقنيات، خصوصًا، الحق في الوصول إلى شبكة الإنترنت أو شبكة الويب العالمية([1]).

ويعَّد الوصول إلى الإنترنت وكذلك المعلومات المفتوحة للجميع، يمكن تناولها بطريقتين مختلفتين: أولهما الوصول إلى الشبكة المادية للإنترنت، والثانية الوصول إلى المعلومات على الإنترنت. وفيما يتعلق بالأول ، فقد أعلن المجلس الدستوري حرية هذا الوصول في قراره الصادر في 10 يونيو 2009، ومع ذلك، فإن هذه الحرية تكون مصحوبة بمسؤولية صاحب الوصول عن الاستخدام المخالف لحقوق الطبع والنشر بالإضافة إلى الالتزام بتأمينه([2]).

وفى هذا يقرر المجلس الدستورى الفرنسى أن الوضع الحالى جعل وسائل الاتصال متاحة للجميع" ومع مراعاة التطور العام لخدمات الاتصال العامة عبر الإنترنت، والأهمية التى تكتسبها هذه الخدمات فى المشاركة فى الحياة الديمقراطية والتعبير عن الأفكار والآراء والتواصل الحر، ولذلك يجب أن تكون حرية الوصول إلى هذه الخدمات متاحة للجميع([3]).

أما بالنسبة للطريقة الثانية، تشمل الوصول إلى المعلومات على شبكة الإنترنت، من خلال حماية المجلس هذا الوصول، فقد اعتبر المجلس، على سبيل المثال، دستورية مواد قانون الملكية الفكرية التي تسمح بحفظها وإتاحتها للجمهور، في شكل رقمي، من الأعمال غير المتاحة التي لم تدخل بعد في النفع العام([4])، الأمر الذى جعل حق الاتصال والوصول إلى الإنترنت ليست ذات قيمة دستورية فحسب، بل واضحها المجلس الدستورى كونها من أعلى حقوق الأنسان لما ترتبط به من حقوق أخرى.

---

([1]) Judgement 12790 of the Supreme Court" Archived December 17, 2015, at the Wayback Machine ., File 09-013141-0007-CO, July 30, 2010.

([2]) « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise." Décision n° 2009-580 DC – 10 juin 2009.

([3]) "en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions, [la libre communication des pensées et des opinions] implique la liberté d'accéder à ces services", Décision 2009-580 DC n° 12.

([4]) Décision n° 2013-370 QPC du 28 février 2014.

فالوصول على نطاق واسع إلى المعلومات في العصر الرقمي يؤدي بشكل خاص إلى زيادة الشفافية التي تعد بلا شك شرطًا أساسيًا لحسن سير النظام الديمقراطي، وبهذا المعنى، تمكن المجلس الدستوري من استخدام فوائد التكنولوجيا الرقمية لتسليط الضوء على بعض الأنشطة التي كانت غير مرئية سابقًا من أجل مكافحة تضارب المصالح والفساد([1]).

وهذا ما تضمنه الدستور اليونانى فى تعديل الصادر عام 2001 فى مادته الخامسة إذ يقرر أن" لكل شخص الحق فى الحصول على المعلومات، وذلك على النحو الذى يحدده القانون، ولا يجوز فرض قيود على هذا الحق، إلا بقدر ما هو ضرورى ومبرر لاسباب تتعلق بالأمن الوطنى، ومكافحة الجريمة، أو حماية حقوق ومصالح أطراف ثالثة" وأضافة المادة حق كل الأشخاص فى المشاركة فى مجتمع المعلومات، وشكل يسمح بسهوله وصول المعلومة إلكترونية، فضلاً عن إنتاجها وتبادلها ونشرها، وذلك كله التزام من جانب الدولة"([2] ).

وفى عام 2000، أطلق البرلمان فى إستوانيا برنامجًا ضخمًا لتوسيع القدرة على الوصول إلى شبكة الإنترنت في مختلف أرجاء الدولة. وتقول الحكومة إن شبكة الإنترنت أمر ضروري للحياة في القرن الحادي والعشرين([3]).

فحرية الإنترنت تتضمن ضمان الحق في التعبير والوصول إلى الموارد والمعلومات الرقمية دون قيود تعسفية، ومع ذلك، تواجه تحديات مثل الرقابة، والحجب، والتشريعات المقيدة التي قد تنتهك هذا الحق.

وعلى المستوى الدولي، تعمل منظمات مثل الأمم المتحدة ومنظمات المجتمع المدني على حماية هذا الحق من خلال مبادرات تعزز الانفتاح الرقمي وتقاوم التمييز الرقمي، على الرغم من ذلك، تتخذ بعض الدول إجراءات رقابية تحد من هذا الحق بدعوى حماية الأمن الوطني، مما يثير مخاوف بشأن انتهاكات الحقوق الأساسية.

---

([1])Les Nouveaux Cahiers du Conseil constitutionnel, https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-nouveaux-cahiers-du-conseil-constitutionnel-n-55-56-juin-2017.

(2) Article 5A1. All persons have the right to information, as specified by law. Restrictions to this right may be imposed by law only insofar as they are absolutely necessary and justified for reasons of national security, of combating crime or of protecting rights and interests of third parties.

2. All persons have the right to participate in the Information Society. Facilitation of access to electronically transmitted information, as well as of the production, exchange and diffusion thereof, constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19.

**([3]) Colin Woodard**: Estonia, Where being wired is a human right, July 01, 2003.

وفى هذا النطاق يقرر القانون الخاص بحماية الأمن السيبرانى فى الصين أن تحمي الدولة حقوق المواطنين والأشخاص الاعتباريين والمنظمات الأخرى في استخدام الشبكات وفقاً للقانون، وتشجع على الوصول إلى الشبكات على نطاق واسع، وترفع مستوى خدمات الشبكات، وتوفر خدمات الشبكات الآمنة والمريحة للمجتمع، وتضمن التداول المشروع والمنظم والحر للمعلومات الشبكية([1]).

ولذلك فأن تعزيز حرية الإنترنت يتطلب توازنًا بين حماية حقوق الأفراد وضمان الأمن القومي، وينبغي على الدول اعتماد سياسات تتيح حرية الاستخدام مع احترام القوانين الدولية والمبادئ الأساسية لحقوق الإنسان وتتوافق مع سيادتها الرقمية.

وتقرر محكمة العدل الأوروبية إن معالجة البيانات الشخصية يجب أن تكون مصممة لخدمة البشرية. وإن الحق في حماية البيانات الشخصية ليس حقًا مطلقًا؛ بل يجب النظر إليه في ضوء وظيفته في المجتمع وموازنته مع الحقوق الأساسية الأخرى، وفقًا لمبدأ التناسب، وتحترم اللائحة العامة لحماية البيانات فى اوروبا جميع الحقوق الأساسية وتراعي الحريات والمبادئ المعترف بها في الميثاق كما هو منصوص عليه في المعاهدات، وخاصة احترام الحياة الخاصة والعائلية، ... وحماية البيانات الشخصية، وحرية الفكر والضمير والدين، وحرية التعبير والمعلومات وحرية ممارسة الأعمال التجارية([2]).

وفى إطار التوافق بين حرية الاتصال بالإنترنت وحماية الدولة لفضائها الرقمى وأمنها القومى أكدت محكمة العدل الأوروبية" أن قانون الاتحاد يستبعد فكرة وضع قوانين من شأنها أن تقييد حركة مرور المعلومات والاحتفاظ بالبيانات المتعلقة بالموقع بشكل عام.

ولكنها فى إطارها للتوافق بين حق الدولة فى أمنها القومى ومواجهة الجرائم السيبرانية وبين حق الأفراد فى سرية البيانات الخاصة بهم عملت مبدأ أن دول الاتحاد يمكن أن تحتفظ بتلك البيانات أن كان هناك تهديد لأمنها القومى، وكان هذا التهديد حقيقى ومتوقع، ولكن اشترطت أن يكون الاحتفاظ بالبيانات لفترة زمنية محددة، ويتم

---

([1]) Article 12: The State protects the rights of citizens, legal persons, and other organizations to use networks in accordance with the law; it promotes widespread network access, raises the level of network services, provides secure and convenient network services to society, and guarantees the lawful, orderly, and free circulation of network information, Cybersecurity Law of the People's Republic of China, Passed November 6, 2016. Effective June 1, 2017.

(2) La Cour de justice de l'Union européenne, Judgment in Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), 24 Sep, 2019.

مراجعة تلك الإجراءات من خلال السلطة القضائية المختصة حتى لا تتعسف جهة الإدارة فى الاحتفاظ بهذه البيانات([1]).

فالسيادة الرقمية هي قدرة الدولة على التحكم بالبنية التحتية الرقمية والبيانات الخاصة بها داخل حدودها الوطنية. وتُعد هذه السيادة جزءًا أساسيًا من مفهوم السيادة الوطنية في العصر الرقمي، وهي أمر حيوي لحماية المصالح الوطنية في البيئة الرقمية.

وتشمل السيادة الرقمية التحكم في البيانات، وتطوير البنية التحتية المستقلة، وضمان الأمن السيبراني. وتُمارس هذه السيادة من خلال قوانين مثل لوائح حماية البيانات (GDPR) في الاتحاد الأوروبي أو قوانين الأمن السيبراني في الصين، وتُعد السيادة الرقمية عنصرًا هامًا لتحقيق الاستقلالية في إدارة الشبكات، حيث تتيح للدول حماية خصوصية مواطنيها ومنع التلاعب أو التجسس، ومع ذلك، فإن السيادة الرقمية قد تؤدي في بعض الحالات إلى قيود على تدفق المعلومات بحرية، مما يثير نقاشات حول تأثير هذه السياسات على حرية الإنترنت.

وهذا ما أكدة قانون الأمن السيبرانى الصينى حيث قرر على أن" يجب على كل فرد ومنظمة تستخدم الشبكات الالتزام بالدستور والقوانين ومراعاة النظام العام واحترام الأخلاق الاجتماعية؛ ويجب ألا يعرضوا الأمن السيبراني للخطر، ويجب ألا يستخدموا الإنترنت للمشاركة في أنشطة تعرض الأمن القومي والشرف الوطني والمصالح الوطنية للخطر؛ ويجب ألا يحرضوا على تقويض السيادة الوطنية، أو قلب النظام الاشتراكي، أو التحريض على الانفصال، أو كسر الوحدة الوطنية، أو الدعوة إلى الإرهاب أو التطرف، أو الدعوة إلى الكراهية العرقية والتمييز العرقي، أو نشر

([1]) Notamment, la CJUE a confirmé que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation. Mais la Cour a nuancé cette position en posant que, dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace. CJUE, 6 octobre 2020, (C-623/17, C-511/18, C-512/18 et C-520/18).

معلومات عنيفة أو فاحشة أو جنسية، أو إنشاء أو نشر معلومات كاذبة لتعطيل النظام الاقتصادي أو الاجتماعي، أو المعلومات التي تنتهك سمعة الآخرين أو خصوصيتهم أو ملكيتهم الفكرية أو غيرها من الحقوق والمصالح المشروعة للآخرين، وغيرها من هذه الأفعال([1]).

ولذلك يجب التوازن بين أمرين؛ أولهما السيادة الرقمية، وثانيهما حق الانسان فى الوصل إلى الإنترنت، ولهذا فأن السيادة الرقمية تُمثل حماية للمصالح الوطنية في البيئة الرقمية. ولكن يجب تحقيق توازن بين حماية البيانات وضمان الانفتاح الرقمي لتجنب تقييد الحريات أو العزلة التكنولوجية.

وتُعد العلاقة بين حرية الإنترنت والسيادة الرقمية علاقة معقدة ومتداخلة، حيث تسعى الدول إلى حماية سيادتها الرقمية مع ضمان عدم انتهاك حقوق الأفراد في استخدام الإنترنت، ومع تزايد الاعتماد على التكنولوجيا، تزداد أهمية هذا التوازن.

فبينما تسعى الدول إلى تطبيق سياساتها السيادية الرقمية، قد تُفرض قيود على حرية الإنترنت بدواعي الأمن الوطني أو حماية البيانات، على سبيل المثال، تلجأ بعض الدول إلى الرقابة وحجب المواقع بحجة الحفاظ على استقرارها الداخلي، لكن هذا الإجراء قد يواجه انتقادات باعتباره انتهاكًا للحرية الرقمية، وفي المقابل، تدعو المنظمات الحقوقية إلى ضمان حرية الإنترنت باعتبارها حقًا أساسيًا، مما يزيد من تعقيد المعادلة، ومن جهة أخرى، هناك محاولات دولية لتحقيق توازن، مثل مبادرات الاتحاد الأوروبي التي تهدف إلى حماية البيانات مع الحفاظ على حرية الإنترنت.

ولهذا يتطلب التوفيق بين حرية الإنترنت والسيادة الرقمية سياسات واضحة وشفافة تحقق المصلحة العامة دون المساس بالحقوق الفردية، وتحقيق هذا التوازن هو التحدي الأكبر في العصر الرقمي.

وتُعتبر حوكمة الإنترنت إطارًا تنظيميًا لتحقيق مثل هذا التوافق، وذلك لانه يشمل مجموعة من القواعد والسياسات التي تهدف إلى تنظيم استخدام الإنترنت على المستويين الوطني والدولي، وتتطلب البيئة الرقمية توازنًا دقيقًا بين حرية الاستخدام

---

([1]) Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they must not endanger cybersecurity, and must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism, advocate ethnic hatred and ethnic discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts.

وضمان الأمن والسيادة الوطنية، وهو ما يتم تحقيقه من خلال قوانين وسياسات حوكمة الإنترنت.

فحوكمة الإنترنت تعتمد على مجموعة من المبادئ التي تسعى إلى ضمان إدارة فعالة للموارد الرقمية وحماية حقوق المستخدمين. تُدار هذه الحوكمة على ثلاثة مستويات:

- **المستوى الدولي.**

ويشمل هذاالمستوى جهود المنظمات الدولية مثل ICANN مؤسسة مسؤولة عن إدارة أسماء النطاقات ونظام عناوين الإنترنت، و ITU (الاتحاد الدولي للاتصالات)، الذى ينظم الاتصالات الدولية ويعمل على تطوير السياسات المتعلقة بالإنترنت، إضفة إلى الأمم المتحدة، والذى من خلالها تقوم بعمل مبادرات مثل منتدى حوكمة الإنترنت (IGF) الذي يوفر منصة للنقاش حول قضايا الإنترنت العالمية.

- **المستوى الإقليمي.**

تلعب التكتلات الإقليمية مثل الاتحاد الأوروبي دورًا رئيسيًا في وضع سياسات شاملة لتنظيم حرية الإنترنت، مثل اللائحة العامة لحماية البيانات (GDPR) وهى مثال على تشريع يوازن بين حماية الخصوصية الفردية وتنظيم تدفق البيانات.

- **المستوى الوطني.**

تختلف التشريعات الوطنية حسب الأولويات والسياسات الداخلية لكل دولة.

ففي الصين، يتم فرض قيود صارمة على المحتوى بموجب قانون الأمن السيبراني، هذا النموذج الصينى يعكس الصراع بين حرية الإنترنت وحاجة الدولة لضمان الأمن الوطني والحفاظ على قيمها الثقافية، مما يجعل حرية الوصول إلى المعلومات مقيدة بشكل كبير، وفي الولايات المتحدة، يتم التركيز على تعزيز حرية الإنترنت مع وجود قوانين تحمي الملكية الفكرية والبيانات، الأمر الذى يجعلها نموذجًا جيدًا للحرية الرقمية، حيث تروج الحكومة الأمريكية لسياسات تدعم حرية الإنترنت وتنظيم المحتوى بما يتماشى مع مبدأ "عدم التدخل"، ومع ذلك، ظهرت قضايا متعلقة بحماية البيانات، مثل فضيحة كامبريدج أناليتيكا، التي أثارت قلقًا حول تأثيرات الشركات الكبرى في مراقبة البيانات الشخصية للمستخدمين، وبالرغم من تمسك الولايات المتحدة بحرية الإنترنت، إلا أنها تسعى لضبط الأنظمة الرقمية في محاولة لحماية المواطنين من التهديدات السيبرانية والمعلومات المضللة.

لذلك تختلف الدول في ترتيب أولوياتها بين ضمان حرية الإنترنت أو فرض السيادة الرقمية، ففي بعض البلدان، تظل السيادة الرقمية أولوية قصوى، بينما في دول أخرى، تُعتبر حرية الإنترنت حقًا أساسيًا يجب الحفاظ عليه.

ويمكن تحقيق التوافق من وجهين الأولى؛ العمل على وضع إطار قانونى وتنظيمى مرن، يسمح بوضع تشريعات وطنية واضحة تحترم حرية الإنترنت، مع ضمان حماية الأمن القومي وسيادة الدول. ويجب أن تكون هذه التشريعات متوافقة مع المعايير الدولية لحقوق الإنسان، إضافة إلى تعزيز فكرة الشفافية والمساءلة، وتشجيع الابتكار الوطنى من خلال الاستثمار في بناء بنية تحتية رقمية وطنية تدعم الشركات المحلية والمبادرات التكنولوجية لتقليل الاعتماد على منصات وشركات أجنبية، وتعزيز القدرات الوطنية في مجال الأمن السيبراني لحماية البنية التحتية الرقمية من التهديدات الخارجية والداخلية دون التضييق على حرية الإنترنت.

والثانية العمل على تعزيز التعاون مع الدول الأخرى والمنظمات الدولية لوضع معايير مشتركة لإدارة الإنترنت، مثل الأمن السيبراني، وحماية البيانات، ومنع الجرائم الرقمية، إضافة إلى وضع قواعد عالمية وسياسات صارمة لحماية البيانات الشخصية للمواطنين، مع ضمان أن تكون البيانات المخزنة داخل حدود الدولة متوافقة مع المعايير المحلية والدولية.

والعمل على توعية المواطنين بأهمية السيادة الرقمية وحقوقهم على الإنترنت لضمان مشاركتهم الفاعلة في تحقيق التوازن بين الحرية والسيادة، وتقليل الفجوة الرقمية بين المناطق الحضرية والريفية لضمان تحقيق العدالة الرقمية، ما يعزز من شرعية سياسات الدولة المتعلقة بالإنترنت.

## المبحث الثانى

## جهود الدول نحو السيادة الرقمية.

إن التكنولوجيات الرقمية، لابد وأن تساهم في تحقيق نتائج مجتمعية أوسع نطاقاً لا تقتصر على المجال الرقمي فحسب، بل لها آثار إيجابية على الحياة اليومية للمواطنين ورفاهتهم وإذا رغبت الدول فى أن تنجح في هذا التحول الرقمي وتحقيق سيادتها الرقمية.

فلابد وأن تسير جنباً إلى جنب مع التحسينات المتعلقة بالديمقراطية والحكم الرشيد والإدماج الاجتماعي والخدمات العامة الأكثر كفاءة.

ولذلك اصبحت البيانات والتقنيات الرقمية عنصرًا أساسيًا في عملية التكامل الأوروبي، فيسعى الاتحاد الأوروبى إلى تعزيز السيادة الرقمية لدية من خلال قدرة الدول الأوروبية على التحكم بمصيرها الرقمية، وتقليل الاعتماد على التقنيات والمنصات الأجنبية.

فالدول تتفاوت فى جهودها نحو السيادة الرقمية بناءً على احتياجاتها وتحدياتها الرقمية، لكنها تشترك فى السعى نحو تحقيق الاستقلال التقنى وفيما يلى نتناول هذه الجهود من خلال ثلاث مطالب على النحو التالى.

المطلب الأول: جهود الدول الأوروبية لتحقيق سيادتها الرقمية.

المطلب الثانى: جهود الصين وروسيا لتحقيق السيادة الرقمية

المطلب الثالث: جهود الدولة المصرية فى تحقيق سيادتها الرقمية.

## المطلب الأول

## جهود الدول الأوروبية لتحقيق سيادتها الرقمية.

أصبحت اليوم التقنيات الرقمية جزءاً لا يتجزأ من الحياة اليومية للأفراد والشركات والمؤسسات في أوروبا، ولكن سوق المنتجات والخدمات الرقمية تهيمن عليه الشركات الأمريكية والصينية متعددة الجنسيات، ولذلك تم تحديد العديد من المخاطر في عدم قدرة أوروبا على التحكم الكامل في بياناتها وبنيتها التحتية الرقمية.

ويُعد تحقيق السيادة الرقمية هدفًا استراتيجيًا للاتحاد الأوروبي، لمواجهة التحديات المتعلقة بالاعتماد على شركات التكنولوجيا الأجنبية وحماية الخصوصية والبيانات، وهناك مجموعة من الاجراءات التي اتخذها الاتحاد الأوروبي لتحقيق السيادة الرقمية، بالإضافة إلى الاجراءات التى اتخذتها الدول الاعضاء لتعزيز سيادتها الرقمية.

**1) على مستوى الاتحاد:**

**أولاً: إصدار اللائحة العامة لحماية البيانات (GDPR):** لحماية الخصوصية والتحكم في البيانات الشخصية فى الاتحاد الأوروبى، وتهدف اللائحة إلى توحيد قوانين حماية البيانات عبر دول الاتحاد الأوروبي، مما يمنح الأفراد سيطرة أكبر على بياناتهم الشخصية، وتنطبق هذه اللائحة على جميع المنظمات، سواء كانت داخل الاتحاد الأوروبي أو خارجه، التي تعالج البيانات الشخصية للمقيمين في الاتحاد الأوروبي، سواء كان ذلك لتقديم سلع أو خدمات أو لمراقبة سلوكهم داخل الاتحاد.

وتتضمن اللائحة متطلبات صارمة، منها:

الحصول على موافقة صريحة من الأفراد قبل جمع أو معالجة بياناتهم الشخصية، وتوفير الشفافية بشأن كيفية استخدام البيانات، وتمكين الأفراد من الوصول إلى بياناتهم وتصحيحها أو حذفها عند الطلب، والإبلاغ عن خروقات البيانات للسلطات المختصة وللأفراد المتأثرين خلال 72 ساعة من اكتشاف الخرق وعدم الامتثال للائحة قد يؤدي

إلى فرض غرامات تصل إلى 20 مليون يورو أو 4% من الإيرادات السنوية العالمية للشركة، أيهما أعلى([1]).

**ثانيًا: إصدار التوجيه (Directive NIS2)** ، ويعتبر هذا التوجيه NIS2 هو تحديث لتوجيه NIS1 الصادر في عام 2016، ويهدف إلى رفع مستوى الأمن السيبراني عبر الاتحاد الأوروبى، دخل حيز التنفيذ في 16 يناير 2023 مع إلزام الدول الأعضاء بتطبيقه بحلول 17 أكتوبر 2024، ويهدف هذا التوجيه إلى تحسين حماية الأنظمة الأساسية والخدمات الحيوية في مختلف القطاعات (مثل الصحة، الطاقة، والنقل)، وتعزيز التعاون بين الدول الأعضاء بالإضافة إلى توحيد متطلبات الأمن السيبراني عبر هذه القطاعات، ويغطي 18 قطاعًا أساسيًا، بما في ذلك الصحة، الطاقة، النقل، البنية التحتية الرقمية، والخدمات المصرفية، ويعمل على تحقيق مستوى عالى من الأمن السيبرانى فى الاتحاد الأوروبى وتوفير تدابير قانونية من خلالها يقوم بفرض التزامات قانونية على الشركات التى تعمل فى هذه القطاعات مما يعزز فكرة السيادة الرقمية لدى الاتحاد الاوروبى([2]).

**ثالثاً: قانون المرونة السيبرانية (Cyber Resilience Act)** صدر هذا القانون في 23 أكتوبر 2024 بهدف تعزيز أمان المنتجات الرقمية (البرمجيات والأجهزة)، وتقليل الثغرات الأمنية في المنتجات الرقمية، والتأكد من أن الأمن السيبراني يُؤخذ بعين الاعتبار أثناء تصميم وإنتاج المنتجات، وتشمل المتطلبات الحد من نقاط الضعف وضمان إدارة الثغرات خلال فترة دعم المنتج ، ويلزم الشركات المصنعة بالإبلاغ عن الثغرات الأمنية التي يتم استغلالها أو الحوادث الكبيرة خلال فترة قصيرة([3]).

**ثالثاً: قانون التضامن السيبراني (Cyber Solidarity Act - CSOA)** يتوقع دخوله حيز التنفيذ في أوائل عام 2025، وصُمم هذا القانون لمواجهة التحديات الناشئة في مواجهة الهجمات الإلكترونية واسعة النطاق، ويعمل على تعزيز التعاون بين الدول الأعضاء لمواجهة الحوادث السيبرانية الكبرى، وتحسين قدرات الكشف والاستجابة للهجمات، من خلال نظام الإنذار السيبراني الأوروبى؛ وهو عبارة عن شبكة من مراكز الأمن السيبراني الوطنية لتوفير التنبيه المبكر عن التهديدات، إلى جانب آلية الطوارئ السيبرانية التى تعمل على توفير إطار عمل لتنسيق الاستجابة للحوادث السيبرانية الكبرى عبر الاتحاد، ووضع آلية لمراجعة للحوادث السيبرانية الكبيرة

---

([1]) (General Data Protection Regulation )GDPR( – Official Legal Text," General Data Protection" ./Regulation )GDPR- September 27, 2022, https://gdpr-info.eu.

([2])**Tambiama Madiega:** Digital sovereignty for Europe, European Parliamentary Research Service, July 2020,P5.

([3]) Report On The State Of Cybersecurity In The Union, Union Agency For Cybersecurity, December 2024, P11

واستخلاص الدروس لتحسين الاستجابة المستقبلية، هذه السياسات تمثل تطورًا كبيرًا في مجال الأمن السيبراني الأوروبي، وتهدف إلى حماية الأنظمة الحيوية، تقليل الثغرات الأمنية، والاستجابة للحوادث السيبرانية بشكل أكثر كفاءة.

وفى سبيل التكريس للسيادة الرقمية للاتحاد الأوروبى ذكرت الوثائق التى تقدم بها مشروع Gaia X والتى نشرته الحكومة الفيدرالية الالمانية عن طريق وزارة الشؤون الاقتصادية والاقتصاد الرقمى، والتى رسخت للسيادة الرقمية بتعريفها بأن السيادة الرقمية هى " إمكانية تقرير المصير بشكل مستقل من قبل الدولة وذلك فيما يتعلق باستخدام الأنشطة الرقمية والبيانات المنتجه والمخزنة فى هذه الأنظمة([1]).

ولهذا حرصت الدول الأوروبية على التفكير فى استعادة السيادة الرقمية الخاصة بها باعتبارها حلاً ممكن للمحافظة على الهوية السياسية والاجتماعية والثقافية لمواطنى الاتحاد الاوروبى، وتحقيقاً لهذه الغاية ظهرت العديد من المبادرات على مستوى الدول الاعضاء والاتحاد كما سنرى لاحقاً.

فالدور المتزايد لشركات التكنولوجيا الاجنبية كانت سبباً للمطالبة بالسيادة الرقمية فى اوروبا، وذلك حفاظاً على السيادة الخارجية لدول الاتحاد وقدرتها على ممارسة سلطتها دون تدخل من كيانات أخرى، ولهذا يُنظر إلى ذلك الآمر كونه تهديداً للمجتمع الرقمى الأوروبى، فالخدمات التى تقدمها هذه الشركات غير الاوروبية تهيمن على السوق، وبالتالى تفرض قواعدها ويترك الافراد والمؤسسات المتعاملة معها تحت وطئة تطبيق هذه القواعد.

بالأضافة إلى سعى الدول الأوروبية إلى المحافظة على خصوصية المجتمع الأوروبى وحماية بياناته الشخصية، فهذه الشركات قد لا تقدم المستوى المطلوب من الحماية، فالاعتماد الكبير على مقدمى الخدمات الاجانب يعرض الأوروبيين لانتهاكات محتملة تؤثر على حياة الأفراد.

ولهذا بدأت دول الاتحاد الأوروبي الحديث عن السيادة الرقمية في أوائل العقد الأول من القرن الحادي والعشرين. وأن كان هناك محاولات لبعض الدول الأعضاء فى الاتحاد الاوروبى فى إنشاء بنية تحتية رقمية وطنية. ففي عام 2011، أطلقت الحكومة الفرنسية مشروع "السحابة السيادية"، Andromèd مما أدى في وقت لاحق إلى ظهور منصتين متنافستين، Cloudwatt التي تديرها شركة أورانج، و Numergy، التي تقود ها شركة SFR ، وفي عام 2013، قدمت شركة Deutsche Telekomمشروعًا لإنشاء"Internetz "، وهو إنترنت ألماني يقوم بتوجيه جميع بيانات حركة المرور على المستوى الوطنى.

---

(1) **Edoardo Celeste**: Digital Sovereignty in the EU: Challenges and Future Perspectives, https://www.bloomsburyprofessional.com/uk/data-protection-beyond-borders

وفي الآونة الأخيرة، شهد إطلاق مشروع Gaia-X الفرنسي الألماني، الذي يدعو إلى إنشاء بنية تحتية سحابية اتحادية أوروبية([1])، اعترافاً بضرورة تجاوز النهج الضيق النطاق والانضمام إلى القوى على مستوى الاتحاد الأوروبي لتقديم بنية تحتية رقمية أوسع وأكثر قابلية للتطوير، ويبدو أن هذا النهج الفيدرالي هو الحل الذي أوصت به مفوضية الاتحاد الأوروبي مؤخرًا ف يبيانها لعام 2020 بشأن استراتيجية الاتحاد الأوروبي للبيانات([2])، وذكرت أنه ستكون هناك مساحة للبيانات الأوروبية نتيجة لتعددية النظم البيئية الرقمية المتوافقة على مستوى الاتحاد الأوروبي، حيث تغطي كل منها قطاعًا بالغ الأهمية من الاقتصاد الأوروبي، ولتحقيق هذه النتيجة لا تخطط المفوضية لاستثمار قدر كبير من الموارد لبناء البنية التحتية اللازمة في العقد المقبل فحسب، بل تهدف أيضا إلى تقديم حزمة تشريعية متماسكة من شأنها أن تكمل الإطار التنظيمي الحالي لحماية البيانات([3]).

هذا وقد بدأت المناقشات أيضًا في أوائل عام 2010، ولكن على المستوى الوطني. ومن الأمثلة البارزة على ذلك فرنسا، حيث كانت السيادة الرقمية في عام 2012 موضوعًا بالفعل على طاولة النقاش، خاصة مع شخصيات مثل بيلانجر ([4]) وآخرين الذين بدأوا يتحدثون عن تطبيق السيادة الرقمية كنوع من المحاولة لتحرير أوروبا من سيطرة الشركات الأمريكية. وكان هناك أيضًا نوع من النقاش في ألمانيا، لكنه كان أكثر ارتباطًا بعلامة يمينية متطرفة وليس باستراتيجية وطنية رحب بها الطيف السياسي بأكمله، وكانت نقطة التحول الحقيقية هي ما كشف عنه سنودن.

هذا لأن أوروبا بدأت تفهم كيف استخدمت الولايات المتحدة هذه التقنيات كسلاح، وفي وقت لاحق، تم وصف السيادة الرقمية بشكل متزايد على أنها قدرة أوروبا على التصرف بحرية واستقلالية في الفضاء الرقمي، وأصبح هذا هو الهدف وراء عدد كبير من السياسات الأوروبية مثل اللائحة العامة لحماية البيانات و أيضًا قانون الذكاء الاصطناعي والآن توجد رغبة حقيقية لدى أوروبا فى أن تكون حره في تقرير مصيرها في الفضاء الرقمي. ولهذا تصبح السيادة الرقمية عنصرًا استراتيجيًا في سياسة أوروبية ، أو على وجه التحديد الاستقلال الاستراتيجي [(5)].

---

(1) Federal Ministry for Economic Affairs and Energy (BMWi), 'Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem' (n 2)

(2) European Commission (n 49) 16.

(3) European Commission (n 49) 12.

(4)) Voir par exemple : Bellanger, Pierre. » De la souveraineté numérique « , Le Débat, vol. 170, no. 3, 2012, pp. 149-159.

**(5) Samuele Fratini**: Quels Sont Les Modèles De Mise En Œuvre De La Souveraineté Numérique ? op. cit.p34.

وإن كانت السيادة الرقمية هى قدرة الدولة القومية على ممارسة السيطرة على كيفية جمع البيانات وتخزينها واستخدامها طوال دورة تدفق البيانات.

ولتحقيق هذه الغاية، بدأ الاتحاد الأوروبي، في استخدام هياكل الحكم التقليدية لفرض سيطرته على البيانات، التى يتم تداولها داخل الاتحاد. فالفكرة المتكرسة هي أنه إذا كان بإمكانك أخذ تلك البيانات وتخزينها في ولايتك القضائية، فسوف تنطبق قوانينك على تلك البيانات، مما يسمح لك بالهروب من ولايات قضائية أخرى تهددك.

ومع ذلك، فمن المهم عدم الحد من القدرة على ممارسة السيطرة على تدفقات البيانات إلى البعد الإقليمي وحده. على سبيل المثال، تمارس الولايات المتحدة درجة عالية من السيادة على البيانات دون اللجوء إلى الولاية القضائية الإقليمية. ففي عام 2018، قدموا قانون USA CLOUD، الذي يسمح لسلطات الولاية بالوصول إلى قواعد البيانات الخاصة في حالة الطوارئ دون الرجوع إلى صاحب البيانات سواء كانت هذه البيانات مخزنة داخل الولايات المتحدة أو خراجها.

في عام ،2013، علق مؤتمر سلطات حماية البيانات الوطنية الألمانية إصدار تراخيص لنقل البيانات من ألمانيا إلى دول خارج الاتحاد الأوروبي، وفي الآونة الأخيرة، وتحديدًا عام 2019 حظر مفوض حماية البيانات وحرية المعلومات في ولاية هيسن في وسط ألمانيا، مؤقتاً استخدام Office Microsoft 365 من قبل المدارس، وادعت هيئة حماية البيانات الوطنية أن قرار مايكروسوفت بتخزين البيانات خارج الاتحاد الأوروبي كان من شأنه أن يعرض المعلومات الشخصية المتعلقة بأطفال هيسن لخطر الوصول إليها من قبل سلطات إنفاذ القانون الأمريكية.

وبالتالي، كان من الممكن تبرير حظر مايكروسوفت للحفاظ على السيادة الرقمية للدولة من خلال ضمان أن مستوى الحماية الممنوحة للبيانات التي تعالجها مايكروسوفت لا يتماشى مع الحقوق الأساسية الأوروبية والألمانية.

وإن ضمان مستوى عالٍ من حمايةالبيانات داخل الاتحاد الأوروبي من خلال تخزين البيانات فعلياً في أراضي الاتحاد، يعني ضمنياً أن الشركات غير الأوروبية تتخلى عن استخدام بنيتها التحتية الرقمية الموجودة في الخارج([1]).

وظهرت العديد من المبادرات على المستوى الوطني ومستوى الاتحاد، من خلال الدعوة إلى إنشاء مثل هذه البنية التحتية، وتتحدث عن عدم كفاية الموارد المتاحة في الاتحاد الأوروبي ، وفي هذا السياق، يستطيع المرء أن يذكر الفكرة ـ المقترحة منذ عام 2011 ـ المتمثلة في السحابة المخصصة للاتحاد الأوروبي أو حتى منطقة الشنجن الافتراضية، وفي عام ،2016 أطلقت المفوضية الأوروبية مبادرة السحابة الأوروبية كعنصر رئيسي في استراتيجية السوق الرقمية الموحدة، ويستلزم هذا

(1) General Data Protection Regulation )GDPR( – Official Legal Text," General Data Protection" ./Regulation )GDPR- September 27, 2022, https://gdpr-info.eu

المشروع إنشاء سحابة علمية أوروبية مفتوحة، وبنية تحتية سحابية آمنة للباحثين، وبنية تحتية أوروبية للبيانات، والتي من شأنها أن توفر حلول الحوسبة الفائقة الأساسية .

وفى 23 فبراير 2022 أصدرت المفوضية الأوروبية قانون البيانات الأوروبى DA وهو قانون من شأنه وضع قواعد لتميكن العادل من الوصول إلى البيانات والاستخدام الأمثل لها، ويسعى هذا القانون إلى إزالة الحواجز من أمام المستهلكين ووصول الشركات إلى هذا البيانات الناتجة عن طريق أجهزة انترنت الأشياء ( IOT)([1]) .

ولتحقيق هذا الهدف يجب وضع مجموعة من القواعد لتحقيق الوصول العادل للبيانات على النحو التالى:

1) يجب العمل على زيادة اليقين القانونى للمستهلكين والشركات التى تنتج البيانات وذلك عندما يتعلق الأمر باستخدام أو نقل هذه اليانات.
2) منع الانتهاكات الناتجة عن الاختلالات التعاقدية التى قد تقوض نقل البيانات.
3) التأكيد على أن هيئات القطاع العام يجوز لها الوصول إلى البيانات التى يحتفظ بها القطاع الخاص واستخدامها اثناء حالة الطوارى العامة أو اتاحتها عن طرق تفويض قانونى أذا لم تكن البيانات متاحة بطرقة أخرى.

---

[1] )شير مصطلحIoT ، أو إنترنت الأشياء، إلى مجموعة من الأجهزة المتصلة والوسائل التكنولوجية التي تيسر الاتصال بين الأجهزة والسحابة، وكذلك بين الأجهزة نفسها. وبفضل ظهور رقائق الكمبيوتر ميسورة التكلفة واتصالات النطاق الترددي العالي، أصبحت لدينا الآن مليارات الأجهزة المتصلة بالإنترنت. وهذا معناه أن الأجهزة التي نستخدمها يوميًا مثل فرش الأسنان والمكانس الكهربائية والسيارات والآلات يمكنها استخدام أدوات الاستشعار لجمع البيانات والتجاوب بذكاء مع المستخدمين .

إن إنترنت الأشياء يُدمج "الأشياء" اليومية مع الإنترنت. يضيف مهندسو الكمبيوتر أدوات استشعار ومعالجات إلى الأشياء اليومية منذ التسعينيات. إلا أن التقدم كان بطيئًا في البداية لأن الرقائق كانت ضخمة وكبيرة الحجم. فقد استُخدمت رقائق كمبيوتر منخفضة الطاقة تسمى علامات RFID لأول مرة لتتبع المعدات باهظة الثمن. ومع تقلص حجم الأجهزة الحاسوبية، أصبحت هذه الرقائق أيضًا أصغر حجمًا وأسرع وأكثر ذكاءً بمرور الوقت.

في الوقت الحالي، انخفضت تكاليف دمج القدرة الحاسوبية في الأشياء الصغيرة انخفاضًا كبيرًا. على سبيل المثال، تستطيع إضافة اتصال مشتمل على إمكانات خدمات Alexa الصوتية إلى وحدات التحكم المصغرة (MCU) التي يقل حجمها عن 1 ميجابايت من ذاكرة الوصول العشوائي (RAM) المدمجة، مثل مفاتيح الإنارة. وقد انطلقت صناعة كاملة تصب تركيزها على ملء منازلنا وشركاتنا ومكاتبنا بأجهزة إنترنت الأشياء. وتستطيع هذه العناصر الذكية نقل البيانات تلقائيًا من الإنترنت وإليه. ويُشار إلى كل هذه "الأجهزة الحاسوبية غير المرئية" والتكنولوجيا المرتبطة بها مجتمعة باسم إنترنت الأشياء. للمزيد راجع:

**Talal Sultan**: Internet Of Things-Iot: Definition, Architecture And Applications, Egypt. J. of Appl. Sci., 34 (1) 2019 P81-95

4) تمكين المستهلكين من التبديل بسهولة بين مختلف مقدمى خدمات معالجة البيانات([1]).

ولذلك فمن الممكن تحديد سلسلة من الآليات الأخرى التي من شأنها أن تساهم في إعادة تأكيدالسيادة الرقمية الأوروبية. على سبيل المثال، يعتبر تشاندر ولي، أن القواعد الخاصة بحماية البيانات في الاتحاد الأوروبي، والتي تحد من نقل البيانات الشخصية إلى دول خارج الاتحاد بمثابة مطالبة بالسيادة الرقمية، على الرغم من أن هذا ليس هدفاً صريحاً للقانون العام لحماية البيانات.

فالنطاق الواسع لتطبيق اللائحةالعامة لحماية البيانات وإدخال غرامات قاسية في حالة انتهاك قواعد حماية البيانات دفع الشركات الأمريكية إلى تبني المعايير الأوروبية الجديدة بشكل استباقي، والذي يشمل أيضاً الشركات غير المؤسسة في أراضي الاتحاد الأوروبي، يمكن اعتباره أيضاً نتيجة طبيعية للسيادة الرقمية الأوروبية([2]).

## المطلب الثانى

## جهود الصين وروسيا لتحقيق السيادة الرقمية

**أولاً: جهود الصين فى تحقيق سيادتها الرقمية.**

تعتبر الصين النموذج الأبرز الذى يسعى إلى الاعتراف بالسيادة الرقمية فى الفضاء الرقمى، فمن خلال القوانين والابتكارات التقنية والمعلوماتية تهدف الصين إلى بناء سيادة رقمية قوية، وتسعى إلى إعادة صياغة المبادئ التى تحكم الفضاء السيبرانى وفقاً لما تراه محققاً لمصالحها الوطنية وترسيخ لسيادتها على الفضاء الرقمى.

فقد كان يُنظر إلى توسع الإنترنت والشبكة العالمية في الصين منذ البداية على أنه مسألة تتعلق بالأمن القومي، ويفسر هذا جزئيًا نموذج مختلف للسيادةلديها: ففي الصين

---

(1) ) Federico Casolari, and others, The EU Data Act in Context: A legal assessment, Digital Ethics Center, Yale University, 2022 , P 3. For more information, 1 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act)', COM(2022) 68 final, 23 February 2022. All EU law documents, including the decisions adopted by the Court of Justice of the European Union, mentioned in this paper are available at https://eur-lex.europa.eu/homepage.html.

(2) Edoardo Celeste: Digital Sovereignty in the EU: Challenges and Future Perspectives, European Studies The Review Of European Law, Economics And Politics, Volume9,Issue 2,P62.

الخط الفاصل بين الشركات الخاصة والسلطات العامة ليس واضحًا كما هو الحال في أوروبا.

ويشكل هذا فارقًا رئيسيًا لأن استراتيجية السيادة الرقمية في الصين لا تتميز بحاجة الدولة إلى إعادة تأكيد سيطرتها على البنية التحتية الرقمية، لأن الفضاء السيبراني لم يكن من المتصور قط أن يكون شخصًا عديم الجنسية في الصين. لقد تم توجيهها دائمًا من قبل الحزب الشيوعي الصيني. وبما أن الصين رأت نفسها كنوع من القوة المناهضة للاستعمار، فقد أظهرت الحاجة إلى أن تكون ذات سيادة، خاصة في مواجهة التوسع للتكنولوجيا الأمريكية والقيم الأمريكية ذات الصلة.

فمنذ أواخر التسعينيات يمكن ملاحظة كوكبة من المبادرات مثل جدار الحماية العظيم أو دعم التعددية في الهيئات الدولية، والتي تصف النهج الصيني في التعامل مع الحوكمة الرقمية باعتبارها قضية إقليمية.

ولذلك يهتم القانون الصيني باتخاذ الاجراءات اللازمة التى تعمل على مراقبة ومنع ومعالجة مخاطر وتهديدات الأمن السيبراني التي تنشأ داخل وخارج أراضي جمهورية الصين الشعبية، وتحمي الدولة البنية التحتية للمعلومات الحيوية من الهجمات والاختراقات والتدخل والتدمير؛ وتعاقب الدولة الأنشطة السيبرانية غير القانونية والإجرامية وفقًا للقانون، وتحافظ على أمن الفضاء الإلكتروني ونظامه([1]).

وتخزين وجميع البيانات الشخصية التي يتم جمعها بواسطة البنى التحتية المعلوماتية الحيوية، مثل الرعاية الصحية والمؤسسات المالية وشركات الطاقة والنقل، يجب أن تتم داخل الأراضي الوطنية([2]).

فالسياسة الرقمية في الصين تعكس توازناً حساساً فبينما كانت الحاجة الصينية لشركات التقنية الأجنبية ضروريًا في مرحلة التسعينات واوائل القرن ال،21 فقد حاولت الاستفادة من القدرات في تطوير أرضية محلية موطنة بدل الاستمرار في الاعتماد على استيرادها ومن مظاهر تطبيق الصين سيادتها الرقمية ما يلى.

**1) قانون التشفير.**

اقترحت لجنة إدارة التشفير الحكومية التابعة لمجلس الدولة 1999مشروع قانون التشفير و عرف باللوائح المتعلقة بإدارة الاستخدامات التجارية للتشفير.

---

([1]) Article 5: The State takes measures for monitoring, preventing, and handling cybersecurity risks and threats arising both within and without the mainland territory of the People's Republic of China. The State protects critical information infrastructure against attacks, intrusions, interference, and destruction; the State punishes unlawful and criminal cyber activities in accordance with the law, preserving the security and order of cyberspace.

([2]) ) W Kuan Hon and others, 'Policy, Legal and Regulatory Implications of a Europe-Only Cloud' (2016) 24 International Journal of Law and Information Technology

و هدف المقترح هو ضرورة تمرير كل منتجات التشفير الاجنبية وأي تكنولوجيا تحتوي عليها الموجه نحو السوق المحلية عبر اللجنة المذكورة. كما حدد المقترح إجراءات تنظيم تقديم مفاتيح التشفير الى الحكومة الصينية .

ومع هذا تبادرت مخاوف للشركات من خطر تهديد ملكيتهم الفكرية جراء الفحص و بعد استيعاب الحكومة الامريكية لكمية المخاطر التي تهدد شركاتها ضغطت لتعديل هذه الشروط و هو ما كان بعد شهر من صدور القانون . و قد يفهم من الانصياع الصيني في هذه الحالة و الفترة هو موقعها للتفاوض المتدني حينها لعدة اسباب منها الافتقار الى الإجماع الداخلي حول تنظيم المنتجات المشفرة داخل الحكومة الصينية إضافة الى الظروف المحيطة بشأن التفاوض بشأن الدخول في منظمة التجارة العالمية و أي تعنت ممكن منها سيعرقل اتمام أمر الانخراط الصيني و مع هذا، فقد تم تنفيذ القانون لاحقًا بشكل جزئي.

**2) تشريع WAPI .**

هذا التشريع كان ينظر إليه كمعيار تقني محلى ففي عام ،2001 قادت معركة بين الحكومة الصينية وشركة SEMC إلى إنشاء معيار تشفير لاسلكي جديد يدعى WAPI. كان الهدف من هذا المعيار تعزيز الأمن وتحقيق الابتكار المحلي، ولكن هذه المبادرة واجهت معارضة من الشركات الأجنبية .ففي نوفمبر ،2003 أعلنت الحكومة الصينية أن جميع الأجهزة التي يمكن الوصول إليها عبر الإنترنت في الصين ستحتاج إلى التشغيل على معيار WAPI بحلول 1 ديسمبر ،2003 مما أثار العديد من التحديات الفنية والاقتصادية للشركات الأجنبية والحكومة فى هذا التوقيت اختارت شركات محلية للحصول على حق الوصول إلىWAPI ، مما جعل الشركات الأجنبية تواجه عقبات في استخدام هذا المعيار الصيني. هذا الصراع عكس توتّرًا بين دعم الأبتكار المحلي والمخاوف من تأثير المعايير الوطنية على الشركات الصينية والعالمية الأمر الذى جعل الصين تتنازل عن هذا المشروع بعد ذلك.

**3) Escort Youth-Dam Green.**

في مايو2009 أصدرت وزارة الصناعة وتكنولوجيا المعلومات الصينية MIIT إشعاًرا يفرض تثبيت برنامج تصفية الويب المسمى "Escort Youth-Dam Green" "مسبقًا على جميع أجهزة الكمبيوتر المباعة في الصين اعتباًرا من 1 يوليو 2009 هذا البرنامج كان يهدف لحظر المواد الإباحية وحماية الأطفال، ولكن هذا التنظيم الواسع أثار اعتراضات كبيرة من شركات التكنولوجيا الغربية ومدافعي حرية التعبير .

تفاجأت هذه الشركات بالإجراء الذي يعقد تصنيعها للتكنولوجيا في الصين، لكن البرنامج حقق نجاحا في المقاهي والمدارس. وكانت هناك توقعات بأن التغطية الجديدة للبرنامج ستؤدي إلى زيادة التكاليف وتقييد الخصوصية والحريات المدنية. هذا الإجراء أحدث صدمة لشركات التكنولوجيا الأجنبية والمحلية، حيث لم تقدم الوزارة توجيهات حول ما يجب فعله مع الأجهزة المستخدمة بالفعل .في صيف ،2009 أعربت غرفة التجارة الأمريكية و22 منظمة أعمال دولية عن احتجاجها لحكومة الصين بشأن إنشاء

السد الأخضر. تلقت الحكومة الصينية مطالب بإعادة النظر في السد الأخضر لما يُزعم أنه تدخل في الشفافية التنظيمية. وبالفعل، توصلت الأختبارات إلى أن البرنامج يمنع المحتوى السياسي الحساس، مما أثار تأكيدات بحدوث تداخل مع حرية التعبير
أظهرت الأبحاث أيضًا تشابهًا كبيرًا بين برنامج السد الأخضر وبرنامج آخر يعرف بـ CyberSitter، الذي أنتجته شركة صغيرة في كاليفورنيا. في النهاية، تم تحديث البرنامج ليزيل تصفية المحتوى السياسي وأعلنت الحكومة الصينية تعليق القانون بعد ضغوط دولية واعتراضات واسعة النطاق من المواطنين الصينيين .وفي النهاية، قررت الحكومة الصينية جعل السد الأخضر إلزاميًا فقط لبعض الأجهزة العامة في المدارس والمكتبات ومقاهي الإنترنت، ووصف وزير MIIT رد الفعل العنيف ضد القانون بأنه "سوء فهم" ناجم عن سوء كتابته.

ولهذا أصبح الأمن السيبراني أولوية قصوى في عهد الرئيس شي جين بينغ، الذي يرأس إدارة الفضاء السيبراني الجديدة في الصين، وقد دعا الصين مرارًا وتكرارًا إلى أن تصبح "قوة إلكترونية تتمتع بقدرات هجومية ودفاعية على قدم المساواة مع الولايات المتحدة و روسيا.

.في نهاية عام ،2014 أعلنت الحكومة الصينية أنه سيتم إصدار قانون يطالب شركات التكنولوجيا الأجنبية التي تزود البنوك الصينية بالبرمجيات والأجهزة بمشاركة كود المصدر الخاص بها كدليل على أنها لا تبني أبوابًا خلفية للتكنولوجيا لإجراء التجسس.

فالقانون السيبراني يعتبر تغييرًا جذريًا في سياسة التكنولوجيا في الصين، حيث تضمن أمورًا سابقة مثل شروط التشفير والقيود على المحتوى الضار عبر الإنترنت. ويعكس القانون أيضا الدعم الضمني للشركاتيين وذلك تبعاً التكنولوجية المحلية، مما يتطلب من الشركات الأجنبية الشراكة مع مزودي تخزين البيانات المحلى وهذا يساعد على توطين البيانات الجديدة، وعلى الرغم من التدخلات الدبلوماسية من سفراء عدة دول والانتقادات الدولية لقوانين الأمن السيبراني، فإن تطبيق القانون ومتطلباته جعلت الشركات تتكيف مع الظروف المحلية.

هذا التكيف يشمل مشاركة شركات تكنولوجيا كبيرة في مشروعات محددة مع شركات صينية، ونقل البيانات إلى مراكز تخزين داخل الصين، والتعاون مع الشركات المحلية لضمان الامتثال للقوانين الصينية.

ووفقاً للصين فإن السيادة السيبرانية، تعنى حق كل دولة فى أن تختار طريقها الخاص فى الفضاء السيبرانى وفقاً للقواعد المحددة لها، ونتيجة لهذا ترى الصين أن ما يجب على العالم أن يشهد فضاءات سيبرانية وطنية، وفق لضوابط تضعها حكومات الدول، وتخضع لمبدأ السيادة الوطنية لكل دولة.

وفى هذا تعارض الصين فكرة الحرية المطلقة للإنترنت، وما ينتج عنها من سيطرة الشركات الأمريكية ونتجة لفكرة الصين حول السيادة الرقمية عملت على تأسيس فضاء رقمى خاص بها.

ويعد قانون الأمن السيبرانى الصادر 2017 والذى وشددت من خلاله على حق الدول ذات السيادة فى وضع قوانين وقواعد لتنظيم الفضاء السيبرانى طبقاً لما يحقق المصلحة العامة للدولة. فقد نص فى مادته الثالثة على أن تواصل الدولة التأكيد على أهمية الأمن السيبراني وتطوير المعلوماتية، وتلتزم بمبادئ الاستخدام النشط والتطوير العلمي والإدارة وفقًا للقانون وضمان الأمن. وتعمل الدولة على تعزيز بناء البنية الأساسية للشبكات والترابط، وتشجيع الابتكار وتطبيق تكنولوجيا الشبكات، ودعم تنمية الكوادر المؤهلة في مجال الأمن السيبراني، وإنشاء نظام كامل لحماية الأمن السيبراني، ورفع القدرة على حماية الأمن السيبرانى([1]).

وفى هذا القانون يشترط أن تقوم الشركات التى تساهم فى البنية التحتية الحيوية للمعلومات بتخزين بياناتها داخل الحدود الصينية، ولهذا يكون محظور على هذه الشركات من مقدمى الخدمة ف الصين أن يقوم بجمع وبيع المعلومات الخاصة بالمستخدمين، وجاء فى مادته الخامس ليوكد على ان تاخذ الدولة التدابير اللازمة لمراقبة ومنع ومعالجة مخاطر وتهديدات الأمن السيبراني التي تنشأ داخل وخارج أراضي جمهورية الصين الشعبية. وتحمي الدولة البنية التحتية للمعلومات الحيوية من الهجمات والاختراقات والتدخل والتدمير؛ وتعاقب الدولة الأنشطة السيبرانية غير القانونية والإجرامية وفقًا للقانون، وتحافظ على أمن الفضاء الإلكتروني ونظامه. بالأضافة الى ترسيخ فكرة حق النسيان الرقمى التى تم تناوله فى هذا البحث سابقاً وهو أن يعطى حق للمستخدم فى المطالبة بحذف المعلومات الخاصة به والتى لدى مقدمة الخدمة وحرصت الصين على التأكيد على مشغلي الشبكات الذين يمارسون الأنشطة التجارية والخدمية اتباع القوانين واللوائح الإدارية واحترام الأخلاق الاجتماعية والتقيد بأخلاقيات العمل والصدق والمصداقية وتنفيذ التزامات حماية الأمن السيبراني وقبول الرقابة من الحكومة والجمهور وتحمل المسؤولية الاجتماعية.

إلى جانب ذلك سعت الصين إلى الأعتماد على التكنولوجيا المحلية من خلال الاستراتيجية الشاملة الصادرة عام 2016 والذى تهدف الى تحقيق الأكتفاء الذاتى التكنولوجى بحلول 2025([2]).

**ثانياً: جهود روسيا فى تحقيق سيادتها الرقمية.**

تشير السيادة الرقمية في روسيا كونها استراتيجية تهدف إلى تحقيق استقلالية الدولة في المجال الرقمي، وتقليل الاعتماد على التكنولوجيا والبنية التحتية الأجنبية، هذه السياسة

([1]) Cybersecurity Law of the People's Republic of China )Effective June 1, 2017( DigiChina,"- DigiChina, August 16, 2022 https://digichina.stanford.edu/work/translation-

[2] سميرة شرايطية، السيادة السيبرانية فى الصين بين متطلبات القوة وضروريات الأمن القومى، المجلة الجزائرية للأمن والتنمية، مجلد 9 ، العدد 16، 2020 ، ص 396 .

اكتسبت زخماً كبيراً خلال السنوات الأخيرة، خاصة في ظل التوترات الجيوسياسية والعقوبات الغربية. فيما يلي أبرز جوانب السيادة الرقمية في روسيا:

**1. تشريعات السيادة الرقمية.**

أصدرت روسيا عدة قوانين تهدف إلى تعزيز سيطرتها على الإنترنت وتحقيق سيادتها على الفضاء السيبرانى، من أبرزها:

**القانون الاتحادي بشأن البيانات الشخصية**

**the Federal Law on Personal Data (No. 152-FZ)**

ويعتبر هذا القانون الفيدرالي الخاص بحماية البيانات الشخصية، هو التشريع الأساسي الذي يحكم جمع البيانات الشخصية ومعالجتها وتخزينها ونقلها في روسيا. تم سنه لأول مرة في عام 2006 وخضع منذ ذلك الحين للعديد من التعديلات، وكان أحدثها في فبراير 2023.

وينطبق القانون الفيدرالي بشأن البيانات الشخصية على نطاق واسع على أي كيان، سواء كان فردًا أو منظمة، يتعامل مع البيانات الشخصية للمواطنين الروس، بغض النظر عن مكان وجودهم.

وهذا يعني أن القانون يمتد إلى **الأفراد Individuals**؛ فإذا ما قام شخص بجمع أو معالجة أو تخزين بيانات شخصية لمواطنين روس بصفته الشخصية، فإنه يخضع للقانون. وقد يشمل هذا، على سبيل المثال، مشاركة معلومات الاتصال الخاصة بسكان آخرين على منتدى مجتمعي أو إدارة شركة صغيرة عبر الإنترنت تتعامل مع بيانات العملاء.

- **المنظمات Organizations**؛ ويشمل هذا كل شيء من الشركات الصغيرة والشركات الناشئة إلى الشركات الكبرى. وأي منظمة، بغض النظر عن حجمها أو صناعتها، تجمع أو تعالج أو تخزن البيانات الشخصية للمواطنين الروس يجب أن تمتثل للقانون. ويشمل ذلك البيانات التي يتم جمعها من خلال مواقع الويب والتطبيقات وتفاعلات العملاء وسجلات الموظفين.
- **المنظمات الأجنبية Foreign organizations**؛ والتى تمارس عملها من الخارج فحتى إذا لم تكن مقيمًا في روسيا، فإن القانون ينطبق عليك إذا كنت تتعامل مع بيانات شخصية لمواطنين روس. وهذا يعني أنه يتعين علي المنظمات

الأجنبية التأكد من أن ممارساتها المتعلقة بالبيانات تتوافق مع القانون، بغض النظر عن لوائح حماية البيانات في بلدها([1]).
ولذلك، فإن نطاق القانون يصل إلى مجموعة واسعة من الأفراد والمنظمات التي تشارك بأي شكل من الأشكال في التعامل مع البيانات الشخصية للمواطنين الروس.
و**البيانات الشخصية التى يحميها هذا القانون؛ هى** أي معلومات يمكن استخدامها لتحديد هوية فرد معين بشكل مباشر أو غير مباشر. ويشمل هذا التعريف الواسع مجموعة واسعة من نقاط البيانات، بما في ذلك:

- **المعرفات الأساسية Basic identifiers**؛ كالاسم، واللقب، وتاريخ الميلاد ومكان الميلاد، والعنوان، ورقم الهاتف، وعنوان البريد الإلكتروني، ورقم جواز السفر، رقم الضمان الاجتماعي.
- **الخصائص الجسدية والبيومترية Physical and biometric** الجنس، العرق، الجنسية، لون الشعر، لون العين، الطول، الوزن، بصمات الأصابع، الحمض النووي.
- **المعلومات المهنية والمالية Professional and financial information:** كالمسمى الوظيفي، والمستوى التعليمي، وتاريخ التوظيف، والراتب، ومعلومات الحساب المصرفي، وسجلات الاستثمار.
- **البيانات عبر الإنترنت والرقمية Online and digital data**؛ كعنوانIP ، ومعرف الجهاز، وبيانات ملفات تعريف الارتباط، وسجل التصفح، واستعلامات البحث، ونشاط وسائل التواصل الاجتماعي، وبيانات الموقع.

بشكل عام، يوفر قانون حماية البيانات الروسي، من خلال قواعده الخاصة واللوائح الإضافية، إطارًا شاملاً لحماية المعلومات الشخصية الحساسة. ويجب على المنظمات التي تتعامل مع مثل هذه البيانات أن تكون على دراية بهذه المتطلبات وأن تنفذ التدابير المناسبة للامتثال للقانون.
وبموجب قانون حماية البيانات الروسي، يتمتع أصحاب البيانات بالعديد من الحقوق للتحكم في معلوماتهم الشخصية وحمايتها. وفيما يلي أهم حقوق أصحاب البيانات بموجب قانون حماية البيانات الروسي؛ الحق في الحصول على المعلومات والوصول إليها (المادة 14)([2])، والحق في الموافقة (المادة 9)([1])،

---

([1])**Alena Epifanova& Philipp Dietrich**; Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World, German Council on Foreign Relations, No1, February 2022,P13.

([2]) Right to Information and Access (Article 14): Data subjects have the right to know about the processing of their personal data. Data controllers are obliged to provide information about the processing purposes, the source of

والحق في التصحيح (المادة 16)([2])، والحق في الحذف (الحق في النسيان المادة (17)([3])، والحق في تقييد المعالجة (المادة 18)([4])، والحق في نقل البيانات (المادة 20.1)([5])، والحق في الاعتراض (المادة 21)([6]).

**وقانون الإنترنت السيادي (2019):**

والتى يهدف إلى إنشاء بنية تحتية داخلية تتيح تشغيل الإنترنت داخل روسيا بشكل مستقل عن الشبكة العالمية في حال حدوث تهديدات خارجية، وهذا القانون يسمح للحكومة الروسية بالسيطرة على المعلومات التي يمكن لمواطنيها الوصول إليها.

---

the data, the methods of processing, and details about third parties with whom the data may be shared.

([1]) Right to Consent (Article 9): Data subjects' consent is required for the processing of their personal data, except in cases stipulated by law. Consent must be voluntary, specific, and informed, and data subjects have the right to withdraw their consent at any time

([2]) Right to Rectification (Article 16): Data subjects have the right to request the rectification of inaccurate or incomplete personal data held by data controllers. Data controllers must take measures to correct the data in a timely manner.

([3])Right to Deletion (Right to be Forgotten) (Article 17): Data subjects have the right to request the deletion of their personal data when the processing is no longer necessary, or when the data subject withdraws their consent. Data controllers must comply with such requests unless there are legal grounds for the data's retention.

([4])Right to Restriction of Processing (Article 18): Data subjects can request the restriction of processing in certain cases, such as disputing the accuracy of the data or objecting to processing. During the restriction period, data controllers are allowed to store the data but not process it further.

([5])Right to Data Portability (Article 20.1): Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format. They may also request the transfer of their data to another data controller.

([6]) Right to Object (Article 21) Data subjects can object to the processing of their personal data, including processing for direct marketing purposes. Data controllers must cease processing the data unless there are legitimate grounds that override the interests, rights, and freedoms of the data subject.

ويفرض هذا القانون على مزودي خدمات الإنترنت تثبيت برامج خلفية تسمح للدولة الروسية بتصفية المحتوى على الإنترنت، وتبرر الحكومة الروسية هذا بإنها تخلق شبكات وطنية تحمي من خلالها بنيتها التحتية على الإنترنت من الهجمات الإلكترونية([1]).

وقد شبه المراقبون التشريع الجديد بـ "جدار الحماية العظيم" في الصين، وفي هذه الحالة، يتم استخدام نوع من التكنولوجيا يسمى التفتيش العميق للحزم، لتفتيش البيانات عبر الإنترنت مما يسمح للحكومة بعرض وإزالة المعلومات التي تراها حساسة أو ضارة، ويتضمن هذا القانون التفتيش العميق للحزم، والذي من شأنه أن يسمح لموسكو بالتحكم فى نشاط المعلومات عبر الإنترنت بنفس الطريقة التي تفعلها بكين.

وهناك اتجاه آخر فى هذا القانون؛ وهو القدرة التي يمنحها للحكومة الروسية على "إيقاف روسيا عن الاتصال بالإنترنت". وسوف يتجلى هذا في فصل الإنترنت الروسي تمامًا عن بقية العالم، وبموجب هذا التشريع، يمكن للحكومة الروسية أن تمنع الوصول المحلي إلى خوادم الإنترنت الدولية، الأمر الذي من شأنه أن يحد من وصول المستخدمين الروس إلى المواقع الإلكترونية والمعلومات التي يوافق عليها الكرملين.

وهناك مجموعة من القوانين الراسخة التى تعزز من فكرة السيادة الرقمية فى رورسيا. على سبيل المثال مجموعة Les lois yaroyava([2])؛ وهى مجموعة من النصوص الفيدرالية المعتمدة في روسيا في عام 2016. والهدف منها هو تعزيز قدرات الدولة في مكافحة الإرهاب. وتسمح هذه القوانين للأمن الداخلي FSB الوصول إلى بيانات المستخدمين والرسائل عبر الإنترنت، ويتضمن البيانات المشفرة، والتى يجب على شركات التكنولوجيا تقديم مفاتيح فك التشفير للسلطات الروسية عند الطلب.

---

([1])Alena Epifanova& Philipp Dietrich; Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World, Op.Cit ,P15..

(2) Les lois yaroyava sont un ensemble de textes fédéraux adoptés en Russie en 2016. L'objectif déclaré est de renforcer les capacités de l'État dans la lutte contre le terrorisme. Ces lois permettent notamment au service de sécurité intérieure FSB d'accéder aux données des messageries en ligne, y compris les données cryptée

**2. تطوير البنية التحتية المحلية.**

تعمل روسيا على إنشاء شبكة إنترنت مستقلة تُعرف باسم "Runet"، تشمل:مراكز بيانات محلية، ونظام خاص لأسماء النطاقات (DNS) يضمن استمرار تشغيل الإنترنت داخلياً.

إضافة إلى توسيع شبكات الألياف الضوئية الوطنية.

**3. بدائل محلية للتكنولوجيا الغربية.**

إنشاء منصات روسية بديلة للشبكات الاجتماعية، مثل (VKontakte) &(Odnoklassniki) وتطوير أنظمة تشغيل محلية مثل "Astra Linux" لتقليل الاعتماد على مايكروسوفت وويندوز، وتعزيز الشركات المحلية مثل (Mail.ru)&(Yandex) لتقديم خدمات تقنية متكاملة.

**وتهدف روسيا إلى تحقيق اكتفاء ذاتي رقمي بحلول السنوات القادمة، مع التركيز على تطوير تقنيات الذكاء الاصطناعي والحوسبة السحابية والتكنولوجيا المالية مما يعزز سيادتها الرقمية.**

**المطلب الثالث**

**جهود الدولة المصرية فى تحقيق سيادتها الرقمية.**

خطت مصر خطوات متسارعة فى بسط سلطتها القانونية والقضائية على فضائها السيبرانى، فشهدت الساحة المصرية فى الأونة الأخيرة نشاطًا ملحوظًا، فى مجال أمن المعلومات والشبكات، وذلك بالتزامن مع الاهتمام الدولى بشأن أمن المعلومات والبيانات، وهذا فى ظل ما تشهده الساحة العالمية من اختراقات للبنية التحتية الرقمية للعديد من الدول نتيجة التطورات المتسارعة فى مجال تكنولوجيا المعلومات.

لهذا سعت مصر إلى تأسيس منظومة حديثة قادرة على حماية أمن الفضاء السيبرانى المصرى، فأتجه المشرع الدستورى إلى الترسيخ للأهمية الفضاء المعلوماتى فقرر فى المادة **المادة 31** على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون".

وقرر فى **المادة 25** الاهتمام بتوعية المواطنين والقضاء على الأمية الرقمية فنص على أن"تلتزم الدولة بوضع خطة شاملة للقضاء على الأمية الهجائية والرقمية

بين المواطنين في جميع الأعمار، وتلتزم بوضع آليات تنفيذها بمشاركة مؤسسات المجتمع المدني، وذلك وفق خطة زمنية محددة".

وفى إطار المحافظة على الحياة الخاصة نص الدستور فى المادة 57 على أن" للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك".

وفى إطار تكامل المنظومة القانونية لفرض سيادة الدولة المصرية على فضائها السيبرانى وبنيتها التحتية الرقمية وأنشطة الأفراد داخل فضائها الرقمى إصدرات السلطة التشريعية العديد من القوانين التى بموجبها تفرض الدولة سيادتها على بياناتها المتداولة فى فضائها السيبرانى فصدر **قانــون مكافحــة الجرائــم الإلكترونية وجرائــم تكنولوجيــا المعلومات المصري رقم 175 لسنة 2018**، والذى نص فى مادته الأولى على أن مع عدم الإخلال بالأحكام الواردة بهذا القانون وقانون تنظيم الاتصالات رقم 10 لسنة 2003 ، يلتزم مقدمو الخدمة بما يأتي :

1) حفظ وتخزين سجل النظام المعلوماتي أو أى وسيلة لتقنية المعلومات ، لمدة مائة وثمانين يوما متصلة . وتتمثل البيانات الواجب حفظها وتخزينها فيما يأتي :
   ( أ ) البيانات التي تمكن من التعرف على مستخدم الخدمة .
   (ب) البيانات المتعلقة بمحتوى ومضمون النظام المعلوماتي المتعامل فيه متى كانت تحت سيطرة مقدم الخدمة البيانات المتعلقة بحركة الاتصال .
   (د) البيانات المتعلقة بالأجهزة الطرفية للاتصال .
   (هـ) أي بيانات أخرى يصدر بتحديدها قرار من مجلس إدارة الجهاز .
2) المحافظة على سرية البيانات التي تم حفظها وتخزينها، وعدم إفشائها أو الإفصاح عنها بغير أمر مسبب من إحدى الجهات القضائية المختصة، ويشمل ذلك البيانات الشخصية لأى من مستخدمي خدمته، أو أي بيانات أو معلومات متعلقة بالمواقع والحسابات الخاصة التي يدخل عليها هؤلاء المستخدمون، أو الأشخاص والجهات التي يتواصلون معها- تأمين البيانات والمعلومات بما يحافظ على سريتها ، وعدم اختراقها أو تلفها([1]).

---

[1] وأضاف القانون العديد من النصوص التى ترسخ لفكرة بسط السيادة الوطنية على الفضاء الألكترونى فنص على جريمة التعدي على أمن شبكات وأنظمة وتقنيات المعلومات: فأقرت المادة 13 من الفصل الأول جريمة الانتفاع بغير حق من خدمات الاتصالات والمعلومات: فإذا أساء شخص استخدام أنظمة الشبكات أو تكنولوجيا المعلومات في الاتصالات أو البث المسموع أو المرئي، فيمكن

وإصدرت الهئية التشريعية **قانون حماية البيانات الشخصية رقم 151 لسنة 2020** يهدف قانون حماية البيانات المصري إلى تنظيم التعامل مع البيانات الشخصية وإدارتها، باستثناء تلك التي يتعامل معها البنك المركزي المصري والجهات التابعة له، ودخل القانون حيز التنفيذ في 15 أكتوبر 2020 مع فترة سماح مدتها 21 شهرًا للشركات للامتثال له ويجب على الشركات تعيين مسؤول الحماية البيانات أو دفع غرامة قدرها 2 مليون جنيه مصري.

كما يتطلب القانون الحصول على ترخيص لمعالجة البيانات والتحكم فيها والتعامل مع البيانات الحساسة والتسويق الإلكتروني ونقل البيانات عبر الحدود. ويمكن أن تؤدي الانتهاكات إلى فرض غرامات شديدة على مراقبي البيانات ومعالجيها، بمن في ذلك المواطنون المصريون والمواطنون الأجانب والأجانب المقيمون في مصر.

وهناك أربعة أعمال تؤدي إلى السجن تشمل: خرق شروط نقل البيانات عبر الحدود، والتعامل مع البيانات الحساسة دون موافقة، وخرق القانون من قبل معالجي البيانات، ومنع ممثلي مراكز حماية البيانات من أداء واجباتهم([1]).

---

أن يواجه الحبس لمدة تصل إلى ثلاثة أشهر وغرامة تتراوح من عشرة آلاف جنيه مصري إلى خمسين ألف جنيه مصري، حسب الجريمة.

وجرائم الغش والتعدي على نظم وتقنيات المعلومات: تحدد المادة 23 من الفصل الثاني من قانون العقوبات المصري عقوبات الجرائم الواقعة على بطاقات الائتمان والخدمات وأدوات الدفع الإلكتروني سيواجه الأفراد المخالفون الذين يصلون إلى بيانات الاعتماد المصرفية أو طرق الدفع الإلكتروني السجن لمدة تصل إلى ثلاثة أشهر وغرامة تتراوح بين 30 ألفا إلى 50 ألف جنيه مصري، وإذا ارتكبت الجريمة للحصول على أموال أو خدمات من طرف ثالث، يمكن الحكم بالسجن لمدة ستة أشهر وغرامة من 50 ألفا إلى 100 ألف جنيه مصري وإذا استولى الشخص على أموال أو خدمات من طرف ثالث، فسيواجه السجن لمدة عام وغرامة قدرها 100 ألف جنيه مصري. والجرائم المتعلقة بانتهاك الخصوصية والمحتوى غير القانوني: تحدد المادة 25 من الفصل الثالث من قانون مكافحة الجرائم الإلكترونية المصري عقوبات انتهاك المبادئ الأسرية، أو بيع البيانات الخاصة دون موافقة، أو إرسال رسائل بريد إلكتروني دون موافقة، أو نشر معلومات أو صور شخصية دون علم وتتراوح العقوبات من الحبس لمدة عام إلى الغرامة من 50 ألف جنيه إلى 200 ألف جنيه. وإذا ارتكبت ضد شخص اعتباري عام. يمكن أن تكون العقوبة مريحًا من الاثنين معا. تعتبر هذه الجرائم حاسمة في قانون مكافحة الجرائم الإلكترونية المصري الذي يعتبرها جرائم كبيره.

[1] بالإضافة إلى هذه القوانين يوجد العديد من التشريعات التى تهدف إلى فرض سيادة الدولة على الشبكات والمعلومات منها قانون تنظيم الاتصالات القومي رقم 10 لسنة 2003 يهدف الجهاز القومي لتنظيم الاتصالات إلى تنظيم قطاع الاتصالات وتطوير ونشر جميع خدماته بما يواكب أحدث التقنيات ويلبي جميع احتياجات المستخدمين بأنسب الأسعار، ويشجع الاستثمار الوطني والدولي في هذا المجال في إطار حرية الوصول .

ويمكن تلخيص الأهداف الرئيسة للهيئة فيما يلي:

1) التأكد من وصول خدمات الاتصالات إلى جميع مناطق الجمهورية.

وعلى الصعيد الدولى؛ انضمت مصر إلى العديد من الاتفاقيات الدولية التى تسعى إلى حماية الفضاء السيبرانى ومواجهة الجرائم السيبرانية والتى تشكل تهددًا لسيادة الدول من هذه الاتفاقيات اتفاقية الاتحاد الإفريقي، بشأن الأمن السيبراني وحماية البيانات الشخصية (اتفاقية مالابو)؛ وتُعد اتفاقية مالابو، التي اعتمدها الاتحاد الإفريقي في عام 2014 بمثابة إطار قانوني لمكافحة الجرائم الإلكترونية وحماية البيانات في إفريقيا فهو يجرم الأنشطة السيبرانية مثل القرصنة والاحتيال وسرقة الهوية، ويضع إجراءات التحقيق والملاحقة القضائية، ويقوض سلطات حماية البيانات. وتؤكد الاتفاقية على التعاون الدولي في مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية.

كما أنها تحدد الأحكام الجنائية المتعلقة بهجمات أنظمة الكمبيوتر، وانتهاكات البيانات والجرائم المتعلقة بالمحتوى، والتدابير الأمنية للرسائل الإلكترونية. هذا، ويمكن أن يؤدي عدم الامتثال لهذه الضوابط إلى فرض عقوبات وغرامات على تكنولوجيا المعلومات والاتصالات([1]).وفي هذا الإطار تشدد الاتفاقية على إنه يجب تثقيف الموظفين حول حماية البيانات. ومراقبتهم بانتظام بحثًا عن الجرائم الإلكترونية وانتهاكات البيانات([2]).

ولإكتمال الإطار التنظيمى للسيادة الرقمية المصرية، تم أنشاء **المجلس الأعلى للأمن السيبرانى** بقرار رئيس مجلس الـوزراء رقم 2259 في ديسمبر 2014 والمعدل بالقرار رقم 1447 لسنة 2015، ويهدف إلى حماية المعلومات والبيانات لـدى

---

2) حماية الأمن الوطني والمصالح العليا للدولة.
3) ضمان الاستخدام الأمثل للطيف الترددي وتعظيم إنتاجه.
4) التأكد من الالتزام بأحكام الاتفاقيات الدولية النافذة والقرارات الصادرة عن المنظمات الدولية والإقليمية المعتمدة لدى الدولة.
5) مراقبة تحقيق برامج الكفاءة الفنية والدراسات الاقتصادية لخدمات الاتصالات المختلفة.

وقانون تنظيم التوقيع الإلكتروني وإنشاء هيئة صناعة تكنولوجيا المعلومات رقم 15 لسنة 2004 ويعد قانون تنظيم التوقيع الإلكتروني أول تشريع في مصر ينظم المعاملات الإلكترونية، بما يضمن حقوق العملاء ومصداقيتهم، فهو يسمح للوسائل الإلكترونية بتحرير المستندات وتبادلها وحفظها مع الحفاظ على الشرعية، وأنشأ القانون هيئة تنمية صناعة تكنولوجيا المعلومات لإحداث نقلة نوعية في صناعة تكنولوجيا المعلومات في مصر وبناء القدرة التنافسية لتصدير تكنولوجيا المعلومات وتطبيقاتها. في السابق، لم تكن الكتابة والتوقيعات الإلكترونية دليلاً صحيحا أمام القضاء.

(1) African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

(2) Egypt - Information And Communications Technology; And Digital Economy - International Trade Administration - Department Of Commerce United States Of America - Retrieved From https://www.trade.gov/country-commercial-guides/egypt-information-and-communications-technology-and- digital-economy.

الجهات الحكومية مع الاهتمام بـإدارات المعلومات والاتـصـالات فى الـوزارات والجهات المختلفة، والتأكد من توافر التمويل الالزم لضمان تنفيذ منظومة الأمن السيبرانى.

ويختص المجلس بوضع استراتيجية وطنية لمواجهة الأخطار والهجمات السيبرانية والإشراف على تنفيذها وتحديثها بالإضافة إلى المهام التالية:

1) اعتماد تحديد البنى التحتية للاتصالات والمعلومات الحرجة في كافة قطاعات الدولة ووضع أطر تقييم ومتابعة تأمين لها في القطاعات المختلفة.
2) اعتماد أطر واستراتيجيات و سياسات تأمين البنى التحتية للاتصالات والمعلومات الحرجة لكافة قطاعات الدولة.
3) وضع خطط وبرامج تنمية صناعة الأمن السيبراني وإعداد الكوادر اللازمة لمواجهة التحديات والمخاطر السيبرانية ووضع إطار للبحث العلمى والتطوير في مجال الأمن السيبراني.
4) التعاون والتنسيق إقليمياً ودولياً مع الجهات ذات الصلة في مجال الأمن السيبراني وتأمين البنى التحتية الحرجة للاتصالات والمعلومات وإعداد توصيات بأية تدخلات تشريعية لازمة للتأمين.
5) وضع المعايير الملزمة لكافة الجهات كحد أدنى لتأمين البنى التحتية الحرجة للاتصالات والمعلومات والزامها بإعداد خطط الطوارئ.
6) وضع آليات رصد المخاطر والمتابعة الدورية للهجمات السيبرانية وتوزيع الأدوار على المستوى الوطني.
7) وضع وتفعيل معايير وآليات لتحديد اعتمادات البنية الموجودة بين عناصر البنية الأساسية الحرجة والقائمين عليها وما يقع خارجها بحيث يتم تجنب التأثيرات المتتالية.
8) إقرار مواصفات الأمن السيبراني القياسية للأنظمة فى مختلف القطاعات وإضافة معايير الجودة السيبرانية.
9) اعتماد توصيف التقويم الأمنى للقائمين على تشغيل البنى التحتية الحرجة للاتصالات والمعلومات.
10) توضع آلية لمتابعة تأمين وحماية المواقع الحكومية الرسمية على الإنترنت([1]).

(1) ويهدف المجلس الأعلى للأمن السيبراني إلى تعزيز الأمن السيبراني في مصر وحماية البنى التحتية الحيوية الحكومية والخاصة من الهجمات السيبرانية المحتملة وقد اتخذ المجلس العديد من القرارات المنظمة لتحقيق هذا الهدف منها؛

أ- إنشاء مركز للرصد والتحليل والاستجابة للحوادث السيبرانية، وتطوير القدرات الوطنية للأمن السيبراني، وتعزيز التعاون الدولي في هذا المجال.

إلي جانب المجلس الأعلى للأمن السيبرانى تم إنشاء المركز الوطنى للاستعداد لطوارئ الحاسبات والشبكات (Cert-EG)([1])، ويهدف إلى تنسيق أمن الفضاء الالكتروني في مصر بهدف تسهيل الكشف والاستجابة ومنع حوادث أمن الفضاء الالكتروني على الإنترنت. ويختص المركز بتقديم الدعم للقطاع الحكومى والمالى.

ومن منطلق تعزيز الثقة فى البنية التحتية للأتصالات والمعلومات وتطبيقاتها وخدماتها فى شتى المجالات الحيوية فى الدولة وتأمينها، من أجل تحقيق بنية رقمية آمنه وموثوقة للمجتمع المصرى، تم وضع الاستراتيجية الوطنية للأمن السيبراني؛ وتتمثل أهمية هذه الاستراتيجية في نقطتين أساسيتين، أولهما هو التصدي للحوادث السيبرانية التي تزايدت من حيث عددها ومصادرها، وثانيهما هو صناعة فرص للسوق المصرية عن طريق بناء كوادر بشرية وتطوير صناعة وطنية تشارك في زيادة إجمالي الناتج المحلي.

وتعمل الاستراتيجية على بناء إطار تشريعى متكامل وتعزيز الشراكة الوطنية من خلال الأستثمار فى الاقتصاد الرقمى، والعمل على بناء دفاعات سيبرانية قوية

---

ب- إصدار الاستراتيجية الأولي الوطنية للأمن السيبراني 2017 - 2021 والتي تناولت المخاطر والتحديات السيبرانية ثم أهم القطاعات الحيوية المستهدفة والعناصر الأساسية لخطورة التهديدات ثم الهدف الاستراتيجي وركائز التوجه الاستراتيجي لمواجهة الاخطار وآلية التنفيذ.

ت- إصدار الاستراتيجية الوطنية للأمن السيبراني 2023 - 2027 وتهدف هذه الاستراتيجية لتوفير البيئة الآمنة لمختلف القطاعات لتوحيد الرؤى الوطنية سعيًا إلى تحقيق فضاء إلكتروني مصرى مؤمن وقادر على الصمود أمام التهديدات والهجمات السيبرانية وتعزيز النمو والازدهار الاقتصادي.

ث- عمل ورعاية العديد من المؤتمرات الخاصة بمجال الأمن السيبراني والأمن المعلوماتي لاستحداث آلية فعالة لمواجهة التهديدات، آخرهم مؤتمر أمن المعلومات والأمن السيبراني (Caisec24) في النسخة الثالثة منه، والذى انتهى إلى اطلاق الاستراتيجية العربية للأمن السيبراني التي أعدتها المنظمة العربية لتكنولوجيات الاتصال والمعلومات (الإيكتوا) لتكون بمثابة خارطة طريق تقتدي بها الدول في وضع وتطوير استراتيجياتها الوطنية للأمن السيبراني، حيث سيجمع هذا المؤتمر أصحاب المصلحة المتعددين من القطاعين العام والخاص إضافة الى العديد من الخبراء في المجال من جميع انحاء العالم للتعرف على سبل المواجهة الحديثة.

كما يشمل برنامج المؤتمر مجموعة متنوعة من الجلسات والورش العملية التي تغطي مواضيع مثل استراتيجيات الأمن السيبراني، وإدارة المخاطر الرقمية، وتقنيات الكشف عن الاختراقات، وأحدث التقنيات في مجال الحماية من الهجمات السيبرانية.

[1] يقدم المركز الخدمات الخاصة بالأنذار المبكر، ومعالجة الحوادث السيبرانية إلى جانب اختبارات الاختراق، وتعمل هذه الاختبارات على الكشف عن أى هجمات إلكترونية والإجراءات الأستباقية التى تتطلب إتخاذها، وجميع التدابير الممكنة لمواجهة أى حوادث أو جرائم تهدد البنية التحتية للمعلومات المصرية.

إلى جانب ذلك يقدم المركز خدمة حماية المعلومات التى تختص بحماية أصول المعلومات فى القطاعات الحيوية من خلال دراسة احتياجاتها ومستويات نضج أمنها السيبرانى.

وقادرة على الصمود أمام أى هجمات سيبرانية على البيانات والمعلومات المصرية، إلى جانب تعزيز التعاون الدولى فى مجال الأمن السيبرانى، ومن الأمور التى تسعى إليها الاستراتيجية العمل على تغيير ثقافة المجتمع حول الأهمية الخاصة بالأمن السيبرانى.

وفى هذا النطاق تسعى مصر بجدية لتحقيق تقدم ملموس فى تطبيق سيادتها الرقمية وضمان الاستقلال التكنولوجى، فالسيادة الرقمية أضحت ضرورة لتحقيق تأمين البنية التحتية التكنولوجية، وحماية بيانات المواطنين الذين يقنطون فى الدولة.

\

**الخاتمة**

ترسيخًا لمفهوم جديد لسيادة الدولة وبسط سيطرتها على حدود جديدة كان ينظر إليها كمساحة خارج قدرة الدول وفضاء رقمى تسعى كل دولة أن تفرض سيادتها القانونية والقضائية عليه، فالتأصيل لفكرة السيادة الرقمية والتى من خلالها يمكن للدولة التحكم في بياناتها الرقمية والبنية التحتية التكنولوجية، بما يضمن حماية معلومات مواطنيها ومؤسساتها. وفي ظل التحديات المتزايدة في هذا المجال، قسمناً هذا البحث إلى فصلين يشتمل كل منهما على مبحثين يتضمن مطلبين؛ تناولنا فى الفصل الأول، والذى جاء بعنوان السيادة الرقمية ومحدداتها، ما هى السيادة الرقمية وتطور مفهوم السيادة من المفهوم الكلاسيكى إلى ما وصل إليه هذا المفهوم فى ظل الثورة المعلوماتية وآثار فكرة العولمة على هذا المفهوم، إضافة إلى تناول محددات فكرة السيادة الرقمية، من خلال التعرض لماهية الفضاء السيبرانى ومكوناته، وكذلك الشركات الخاصة العاملة فى هذا الفضاء وأثر ذلك على بيانات الأفراد. والتنظيم القانونى للسيادة الرقمية، ودور القضاءين الدستورى والإدارى فى الترسيخ لفكرة سيادة الدولة الرقمية.

ثم تعرضنا فى الفصل الثانى لتحديات التى تواجه تطبيق السيادة الرقمية، والإشكاليات القانونية والاقتصادية التى تواجه فكرة السيادة الرقمية، وكيفية تحقيق التوافق بين مبدأ حرية الإنترنت كمبدأ دستورى وتطبيق الدولة لسيادتها الرقمية، جهود الدول نحو السيادة؛ مثل الاتحاد الأوروبى والصين وروسيا، ثم أخيراً الجهود المبذولة من جانب الدولة المصرية فى تحقيق سيادتها الرقمية.

من خلال هذا العرض خلصنا إلى مجموعة من النتائج والتوصيات.

**1) النتائج:**

- ❖ أن المفاهيم القانونية ليست فى عزلة عن التطورات التكنولوجية، فالثورة الحاصلة فى المجال التكنولوجى له أثر على تغير العديد من المفاهيم، تحت مظلة العولمة، فالثورة المعلوماتية والتكنولوجية شكلت مفهوم جديدًا للسيادة الدول بحيث تسعى الدول إلى بسط سيادتها على الفضاء السيبرانى.
- ❖ ترسيخ مفهوم السيادة الرقمية يتطلب تحديد ثلاث عوامل رئيسية وهما الفضاء السيبرانى المحيط التى تفرض الدولة سيادتها عليه، والشركات الخاصة المنوط بها الالتزام بهذا القانون، والافراد الحريصون على حماية بياناتهم فى هذا الفضاء.
- ❖ لتحقيق السيادة الرقمية ينبغى على الدول التقليل من الاعتماد على مزودى الخدمات الذين قد يشكلون تهديد لهذه السيادة.
- ❖ يجب تعزيز منظومة الأمن السيبرانى لحماية البيانات الوطنية والشبكات الحيوية من الهجمات الإلكترونية، وضمان معالجة هذه البيانات داخل الحدود الوطنية أو الأقليمية وفقًا للقوانين المحلية.
- ❖ تعمل السيادة الرقمية على تقوية الهوية الثقافية الوطنية من خلال انتاج محتوى رقمى يعكس القيم والمبادئ الوطنية، ومنع الهيمنة الثقافية من القوى الأجنبية.

**2) <u>التوصيات.</u>**

- ➢ لتحقيق الدول سيادتها الرقمية عليها تطوير البنية التحتية الرقمية الوطنية، وأنشاء محتوى رقمى وطنى تستطيع من خلاله الحفاظ على تراثها الثقافى والاجتماعى، والحفاظ على هويتها القومية، إضافة إلى إنشاء مراكز بيانات وطنية لتخزين المعلومات الحساسة وضمان حمايتها من الاختراقات الخارجية.
- ➢ تعزيز القدرات في مجال الذكاء الاصطناعي والأمن السيبراني لحماية الدول من الهجمات السيبرانية والتصدى لاى محاولة لتهديد مجالها الرقمى، وإنشاء مراكز متخصصة تحت إشراف هيئات عليا لتطوير الخبرات المحلية في هذه المجالات، لتحقيق الاستقلال الرقمى وعدم الاعتماد على جهات خارجية.

- وضع سياسات وتشريعات لحماية البيانات الشخصية، والتنسيق بين القوانين على المستوى العربي لضمان حماية المعطيات الشخصية وتعزيز التعاون الإقليمي في هذا الشأن.
- التفاوض مع المنصات الرقمية العالمية، وتشكيل فرق عمل للتفاوض مع شركات الإعلام الدولية لضمان حقوق الدول في التحكم بالمحتوى الرقمي وحماية الثقافة المحلية، وعدم فرض محتويات من شأنها الاخلال بالمصالح العليا للدولة، والأمن القومى الاجتماعى.
- تشجيع الابتكار وريادة الأعمال في المجال الرقمي، ودعم المبادرات المحلية لتطوير تقنيات ومنصات رقمية تعزز الاستقلالية الرقمية وتقلل الاعتماد على الحلول الخارجية.
- العمل على التعاون الإقليمي والدولي، لتعزيز التعاون مع الدول الأخرى لتبادل الخبرات واختيار أفضل الممارسات في مجال تحقيق الدول لسيادة الرقمية.
- مازال مجال الأمن السيبرانى والذى يُعد محور السيادة الرقمية فى مراحلة الأولى، لذلك يجب العمل على دمج برامج الأمن السيبرانى فى مناهج المراحل التعليمية المختلفة، وذلك للعمل على زيادة التوعية حول حماية البيانات والمعلومات الشخصية والمؤسسية لدى أفراد المجتمع.

**المراجع والمصادر:**

**أولاً: مراجع باللغة العربية.**


1. **احمد محمد محمد عبد الغفار:** مبدأ السيادة الرقمية الفردية على البيانات، مجلة البحوث الفقهية والقانونية، العدد 43، كلية الشريعة والقانون، جامعة دمنهور، 2023.
2. **أنديراَعراجي:** القوة في الفضاء السيبراني ؛ فصل عصري من التحدي والإستجابة، 2015.
3. **إيجر امنية:** السيادة الرقمية فى العالم المعولم: التحديات والرهانات، مجلة الدراسات القانونية والسياسية، الجزائر المجلد 10 عدد2 يونيو 2024

4. **ثروت بدوى**: النظم السياسية، دار النهضة العربية، بدون تاريخ نشر،
5. **جان جاك روسو**: العقد الاجتماعي، ترجمة عادل زعيتر ، د.ن.
6. **حامد سلطان وآخرون**: الوضع التاريخى لمبدأ السيادة، دار النهضة العربية، 1987.
7. **حسن سمير:** الثورة المعلوماتية عواقبها وآفاقها، مجلة الجامعة دمشق، المجلد 18، العدد 1، 2002،
8. **حسين أحمد مقداد:** دور الضبط الإدارى في الحد من مخاطر الفضاء الإلكترونى فى مصر وفرنسا، مجلة العلوم القانونية والاقتصادية ، العدد الأول ، السنة الخامسة والستون ، يناير 2022،
9. **رغدة البهي:** الوكالة السيبرانية.. عوامل النشأة وأنماط الفواعل، مجلة السياسة الدولية، ملحق اتجاهات نظرية، العدد 218، أكتوبر 2019.
10. **زديك الطاهر &العربي رزق الله بن مهيدي**: العولمة وتقويض مبدأ السيادة ، مجلة الباحث، عدد 2، 2003،
11. **زغو محمد:** أثر العولمة على الهوية الثقافية للأفراد والشعوب، الأكاديمية للدراسات الاجتماعية والإنسانية. 4 – 2010.
12. **سعاد الشرقاوى**: القانون الدستورى والنظم السياسية، بدون دار نشر، 2007.
13. **سلاوي بشرى و أخرين**: مستقبل السيادة الرقمية في ظل التكنولوجيات الحديثة دراسة تحليلية استشرافية، كلية العلوم الإنسانية والاجتماعية، 2020.
14. **سميرة شرايطية:** السيادة السيبرانية فى الصين بين متطلبات القوة وضروريات الأمن القومى، المجلة الجزائرية للأمن والتنمية، مجلد 9 ، العدد 16، 2020.
15. **عبد الفتاح ساير:** القانون الدستوري – النظرية العامة للمشكلة الدستورية- ماهية القانون الدستوري الوضعي، دار الكتاب العربى، الطبعة الثانية، 2004.
16. **عبد الهادى فوزى العوضى:** الحق فى الدخول فى طى النسيان على شبكة الإنترنت، دراسة قانونية تطبيقية مقارنة، دار النهضة العربية، 2014.
17. **عوض المر:** الرقابة القضائية على دستورية القوانين فى ملامحها الرئيسية ، مركز رينيه جان دبوى للقانون والتنمية بفرنسا، 2003.
18. **محمد حمشي و عادل زقاغ:** عن السياسة ما بعد الدولية :تعايش بين نظامين أم عصر وسيط جديد؟، مجلة سياسات عربية، العدد54، مجلد 10، يناير 2022.
19. **محمد عرفان الخطيب**: ضمانات الحق في العصر الرقمي من تبدل المفهوم .. لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي وإسقاط على الموقف التشريعي الكويتي، مجلة كلية القانون الكويتية العالمية، ملحق خاص – العدد3 - الجزء الأول - مايو 2018.

20. **منى الأشقر جبور، ود محمود جبور:** البيانات الشخصية والقوانين العربية: - الهمّ الأمني وحقوق الأفراد، المركز العربى للبحوث القانونية والقضائية، 2018،
21. **مها رمضان محمد بطيخ:** الإطار القانوني للحق في النسيان عبر شبكة الإنترنت، مجلة الدراسات القانونية العدد الحادى والستون – الجزء الاول – يونيو 2020.
22. **هشام عوض احمد**: سيادة الدولة بين مفهومها التقليدى وظاهرة التدويل، جامعة الشرق الاوسط ، الاردن، يونيو، 2013.
23. **ئالان حمه سعيد صالح ،د. عبدالرحمن كريم درويش**: تأثير العولمة على سيادة الدولة، دراسة مقارنة، مجلة القانون والسياسية، 2016.

**ثانياً: باللغة الأجنبية.**

1. **Abdifatah Ahmed Ali Afyare**: The impact of globalization on state sovereignty, International Journal of Science and Research Archive ( IJSRA) 2024, 12(02), P 1653–1662. Article DOI: https://doi.org/10.30574/ijsra.2024.12.2.1434
2. **Ananya Gautam& Shalini Saxena**: The Impact of Globalisation on the National Sovereignty: A Comparative Study, International Journal for Multidisciplinary Research, Volume 6, Issue 2, March-April 2024.
3. **Annie Blandin-Obernesser**: Les entreprises souveraines de l'Internet : un défi pour le droit en Europe., Droits et souveraineté numérique en Europe, Bruxelles, Bruylant.
4. **Annie I. Anton & Travis D. Breaux:** Digital privacy: theory, policies and technologies, Article in Requirements Engineering · March 2011.
5. **Alena Epifanova& Philipp Dietrich**; Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World, German Council on Foreign Relations, No1, February 2022,P13.
6. **Asif Raihan**: A review of the potential opportunities and challenges of the digital economy for sustainability,

Innovation and Green Development, Volume 3, Issue 4, December 2024.

7. **Baezner, Marie; Robin, Patrice**: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS), ETH Zürich , November 2018.
8. **Cf. Edoardo Celeste**: 'Digital Constitutionalism: A New Systematic Theorisation' 33 International Review of Law, Computers & Technology(2019).
9. **Christian Katzenbach and Thomas Christian Bächle:** Digital sovereignty, nternet Policy Review, Volume 9 , Issue 4, : 17 December 2020.
10. **Colin Woodard**: Estonia, Where being wired is a human right, July 01, 2003.
11. **Daniel Castro and Alan McQuinn**: Cross-border data flows enable growth in all industries, Information Technology and Innovation Foundation. Referred to the McKinsey Global Institute (MGI), Digital Globalization: The New Era Of Global Flows, February 2015.
12. **Daniel T. Kuehl**: "From Cyberspace to Cyberpower: Defining the Problem," Cyberpower and National Security, (Washington, DC: Potomac Books, 2009).
13. **E. Geffray**: « Droits fondamentaux et innovation : quelle régulation à l'ère numérique ? », Nouveaux Cahiers du Conseil constitutionnel, n° 52, 2016
14. **Edoardo Celeste**: Digital Sovereignty in the EU: Challenges and Future Perspectives, https://www.bloomsburyprofessional.com/uk/data-protection-beyond-borders
15. **Federico Casolari, and others**: The EU Data Act in Context: A legal assessment, Digital Ethics Center, Yale University, 2022 , https://eur-lex.europa.eu/homepage.html.
16. **Gary Jeffrey**: Constitutional Identity, The Review of Politices 68, 2006.

17. **Grégoire Germain et Paul Massart:** Souveraineté Numérique, Revue Études, N° 10 , Octobre 2017. https://Www.Cairn.Info/Revue-Etudes-2017-10-Page-45.Htm
18. **Falque Pierrotin:** « La constitution et l'Internet », Nouveaux cahiers du Conseil constitutionnel, n° 36, 2012.
19. **Jean Boodin**: six books of the commonwealth translated by m. tooley, basil black well, oxford, Dictinnaire la rouse 2010 P 25.
20. **Jean-Luc Warsmann, Philippe Latombe**: Rapport D'information, Déposé, En Application De L'article 145 Du Règlement Par La Mission D'information Sur Le Thème « Bâtir Et Promouvoir Une Souveraineté Numérique Nationale Et Européenne' N° 4299 Assemblée Nationale , Enregistré À La Présidence De l'Assemblée Nationale Le 29 Juin 2021,
21. **Jens Bartelson**: The Concept Of Sovereignty Revisited, The European Journal Of International Law Vol. 17 No.2,
22. **John Perry Barlow**: A Declaration of the Independence of Cyberspace, Davos, Switzerland, February 8, 1996.
23. **Jorge Emilio Núñez**: "About the Impossibility of Absolute State Sovereignty: The Middle Ages, International Journal for the Semiotics of Law., Volume 28, Issue 2, June 2015.
24. **Jukka Ruohonen:** The Treachery of Images in the Digital Sovereignty Debate, Minds and Machines (2021).
25. **Julia Pohle:** Digital sovereignty A new key concept of digital policy in Germany and Europe, Konrad-Adenauer-Stiftung e. V. Berlin. 2020.
26. **Kévin Deniau:** Cambridge analytique: tout comprendre sur la plus grande crise de l'histoire de Facebook" , available at:

https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/15/02/2020

27. **Krasner D. St: Sovereignty**: Organized Hypocrisy. Princeton: Princeton University Press, 1999.
28. **Luciano Floridi**: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Philosophy & Technology (2020).
29. **Madhuvanthi Palaniappan:** Cyber Sovereignty: In Search of Definitions, Exploring Implications, Issue Brief ISSUE NO. 602 December 2022.
30. **Marin Brenac:** La souveraineté numérique sur les données personnelles Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique**,** Mémoire Maîtrise en droit, Université Laval Québec, Canada Maître en droit (LL.M.)
31. **N. Lucchi**: "Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression", Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011.
32. **Norbert Wiener**: Cybernetics or control and communication in the animal and the machine, second edition, the Massachusetts Institute of Technology Press, Cambridge, England, 1984.
33. **Pierre Bellanger:** La Souveraineté Numérique, Les Dîners De L'institut Diderot.

34. **Pierre-Yves Quiviger**: Une approche philosophique du concept émergent de souveraineté numérique, Nouveaux Cahiers du Conseil constitutionnel n° 57 (dossier : droit constitutionnel à l'épreuve du numérique) - octobre 2017.
35. **Rain Ottis, Peeter Lorents**: Cyberspace: Definition and Implications, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia,
36. **Ramona Gabriela& Adela MoișI**: The Concept Of Sovereignty, Journal of Public Administration, Finance and Law, Issue24, 2022.
37. **Romina Bandura, Madeleine McLean, and Sarosh Sultan:** Unpacking the Concept of Digital Public Infrastructure and Its Importance for Global Development, December 20, 2023, https://www.csis.org/analysis/unpacking-concept-digital-public-infrastructure-and-its-importance-global-development
38. **Samuele Fratini:** Quels Sont Les Modèles De Mise En Œuvre De La Souveraineté Numérique ? [Entretien] 11 juin 2024, https://www.sciencespo.fr/public/chaire-numerique/2024/06/11/entretien-quels-sont-les-modeles-de-mise-en-oeuvre-de-la-souverainete-numerique-par-samuele-fratini/
39. **Stephane Couture& Sophie Toupin**: What does the notion of "sovereignty" mean when referring to the digital?, new media & society, Vol. 21,2019.
40. **Stephen D. Krasner**: Problematic Sovereignty: Contested Rules and Political Possibilities, Columbia University Press, 2001.
41. **Talal Sultan**: Internet Of Things-Iot: Definition, Architecture And Applications, Egypt. J. of Appl. Sci., 34 (1) 2019.

42. **Tom Sorell**: Hobbes on Sovereignty and Its Strains, https://www.researchgate.net/publication/357139416
43. **Valentine Martin**: La République Numérique En Débat Au Parlement : Le Projet De Commissariat À La Souveraineté Numérique, Les Nouveaux Cahiers Du Conseil Constitutionnel - N° 57, Octobre 2017.
44. **Vassilys Fourkas:** What is 'cyberspace'? March, 2004, https://www.researchgate.net/publication/32892863
45. **Vladimir Korovkin**: International Regulation In Cyber Space: Is Effective Mutual Understanding Possible?, January 2022 URL: https://sns-journal.ru/en/archive/
46. **W Kuan Hon and others:** 'Policy, Legal and Regulatory Implications of a Europe-Only Cloud' (2016) 24 International Journal of Law and Information Technology

**المواثيق والدساتير:**

1) الاعلان العالمى لحقوق الأنسان.
2) الاعلان العالمى لحقوق الإنسان والمواطن.
3) دستور جمهورية مصر العربية.
4) دستور الجمهورية الفرنسية.
5) دستور الولايات المتحدة الأمريكية.
6) القانون الأساسى الإلمانى.
7) دستور الهند.
8) دستور اليونان.
9) دستور استونيا.

**المواقع الإلكترونية:**

**https://www.conseil-constitutionnel.fr/**
**https://egcert.eg/ar/**
**https://mcit.gov.eg/ar/Publication/Publication_Summary/10492**
**https://www.cc.gov.eg/**
**https://gdpr-info.eu**
**https://digichina.stanford.edu/work/translation**
**https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection**

الفهرس