

السيادة الرقمية Digital Sovereignty

فرعون محمد

جامعة جيلالي اليابس، سيدي بلعباس / الجزائر
مخبر المرافق العمومية والتنمية
maitrefaraoun@hotmail.com

بلحاج خالدية

جامعة جيلالي اليابس، سيدي بلعباس / الجزائر
مخبر المرافق العمومية والتنمية
Khaldia.belhadh@univ-sba.dz

تاريخ النشر: 2025/07/06

تاريخ القبول: 2025/07/01

تاريخ الإرسال: 2025/05/11

الملخص:

التطور التكنولوجي الهائل في مجال الاتصالات لا سيما بعد رقمنة كافة المجالات والقطاعات لم يحدث تغيرا في طرق العيش فقط، بل تعداها إلى إحداث تغيرات في المفاهيم أيضا، حيث أصبح لها أوجه رقمية، ما جعل المعلومات تنتقل بين الدول في يسر تام، ما جعل الدول أمام خطر محقق بأمها القومي وتحدي كبير لمواجهة التهديدات السيبرانية، وعليه أصبحت السيادة الرقمية جانب رقمي أطلق عليه "السيادة الرقمية" والمحافظة عليها لم تعد اختيار بل ضرورة حتمية لضمان الاستقرار وحرية القرار السياسي والاقتصادي والاجتماعي للدول، كون الهجمات السيبرانية أصبحت عبارة عن هجمات منظمة وممنهجة تحاك ضد الدول قصد تدمير وفرض توجهات وايدولوجيات معينة، وموضوع السيادة الرقمية ذو أهمية بالغة لذا تناولناه في هذه الورقة البحثية بدراسة الجانب المفاهيمي وصولا إلى الجهود التي ما فتئت الدول تبذلها قصد تكريس الحماية اللازمة لها مرور ببعض الصور التي تعد مساسا بها.

الكلمات المفتاحية: الرقمنة – السيادة الرقمية – آليات الحماية.

Abstract:

The tremendous technological advancement in the field of communications—particularly following the digitization of all sectors and domains—has not only transformed lifestyles but also altered fundamental concepts, many of which have taken on digital dimensions. This transformation has enabled the seamless flow of information across borders, thereby exposing nations to imminent threats to their national security and posing significant challenges in addressing cyber threats. Consequently, digital sovereignty has emerged as a crucial dimension known as “digital sovereignty.” Preserving it is no longer a matter of choice but a vital necessity

to ensure national stability and the freedom of political, economic, and social decision-making. Cyberattacks have evolved into systematic and organized campaigns orchestrated against states with the aim of promoting and imposing certain ideologies and agendas, Given the critical importance of digital sovereignty, this research paper explores the conceptual framework of the issue and examines the various efforts made by states to establish the necessary safeguards, highlighting examples of violations that compromise digital sovereignty.

Keywords: Digitization – Digital Sovereignty – Protection Mechanisms.

المقدمة:

شهدت مجالات الحياة على اختلافها، طفرة تكنولوجية هائلة، جعلت من العالم رغم اتساع رقعته قرية صغيرة تنتقل فيه المعلومات بسرعة البرق، وأصب له جزء افتراضي، تغيرت فيه المفاهيم والمصطلحات عنها في جزئه الواقعي الملموس، ومن بين هذه المصطلحات "سيادة الدول" التي أصبح لها وجه رقمي يعبر عن مد قوتها التكنولوجية وقدرة تحكمها في بناها الإلكترونية.

وإن كانت سيادة الدول بشقها الواقعي قد تنتهك بمجرد التدخل في شؤونها الداخلية، ما يؤدي إلى زعزعة استقرارها، فإن سيادة الدول بشقها الافتراضي والتي سميت مجازا بالسيادة الرقمية هي أيضا قد تكون عرضة للانتهاك بعدد الأساليب والطرق، ما يؤدي أيضا إلى المساس بأمنها القومي لذا سعت الدول إلى إيجاد آليات قصد حماية سيادتها في هذا الجانب وعليه نبحت في موضوع السيادة الرقمية للإجابة على الإشكال التالي: "ما مدلول السيادة الرقمية، وما هي الآليات التي انتهجتها الدول لمحماتها؟"

حيث تم اتباع الخطوة التالية:

المبحث الأول: مفهوم السيادة الرقمية للدول.

المطلب الأول: تعريف السيادة الرقمية.

المطلب الثاني: السيادة الرقمية وبعض المصطلحات المشابهة لها.

المبحث الثاني: آليات حماية السيادة الرقمية.

المطلب الأول: صور الاعتداء على السيادة الرقمية.

المطلب الثاني: جهود الدول لحماية سيادتها الرقمية.

الخاتمة.

وذلك وفق المنهج التحليلي الوصفي مع بروز المنهج التاريخي لعرض بعض المعلومات.

السيادة الرقمية

المبحث الأول: مفهوم السيادة الرقمية

يعد مصطلح السيادة الرقمية مصطلحا حديثا كثر تداوله مع التطور التكنولوجي الهائل لوسائل الاتصال والدور الفعال الذي أضحت تلعبه لا في تقريب الشعوب بعضها ما جعل العالم قرية صغيرة بل في توجيه الرأي العام والتأثير على سياسات الدول، وعليه لكي نبث في مفهوم السيادة الرقمية ينبغي البحث في تعريفها مع التعرّج على بعض المصطلحات المتقاربة معها.

المطلب الأول: تعريف السيادة الرقمية

مصطلح السيادة الرقمية يجمع بين لفظين قد يتبادر للوهلة الأولى أنها ينتميان إلى عالين أو مجالين مختلفين ومنفصلين تماما، حيث أن السيادة كمصطلح يمكن إدراجه ضمن اهتمامات العلوم السياسية أو القانونية بينما تعد الرقمنة إحدى اهتمامات العلوم التكنولوجية الحديثة لذا سوف نتطرق إلى تعريف مختصر — لكل المصطلحين على حدى (السيادة والرقمنة) على أن نفصل في مدلول السيادة الرقمية.

أولا: السيادة:

هي لفظ مشتق من فعل ساد سيد وسيادة ويقصد بها الهيمنة والغلبة والسلطة وحرية التصرف.¹ والسيادة هي إحدى الخصائص الجوهرية المرتبطة بالدولة الحديثة كتنظيم سياسي وكيان قانوني، حيث تمتاز بأنها مطلقة شاملة وغير قابلة للتنازل أو التجزئة.²

ويعد المفكر "جون بودان" من الأوائل الذين تناولوا هذه الفكرة في سنة 1576 ليتدرج مفهوم السيادة فيما بعد من منظور ديني إلى قومي وصولا إلى سيادة الشعب ممارستها من خلال دولة منظمة تفرض سلطتها على إقليم معين يعد الحيز المكاني لسيادتها الوطنية، هذه السيادة التي اتسمت إلى حد ما بالحدودية والتقيّد بأداء التزاماتها الدولية من جهة وعلى تصرفها بمطلق حريتها على المستوى الداخلي من جهة ثانية.

ثانيا: الرقمنة:

هي نسبة إلى كلمة "رقم" وهي طريقة لتحويل المعطيات والمعلومات إلى أرقام عادة صفر للسليبي وواحد للإيجابي وتخزينها داخل ذاكرة الحاسب الآلي ما يسهل تنقلها عن طريق الشبكة العنكبوتية.³

¹ - موقع المعاني <https://www.almaany.com.ar.ar> تعريف السيادة في معجم المعاني الجامع، معجم عربي عربي، تاريخ الزيارة 2023/02/17 الساعة 18:54 سا.

² - حمياز سمير، محاضرات حول إشكالية مفهوم السيادة الوطنية في ظل المتغيرات البولية الراهنة، قسم العلوم السياسية والعلاقات الدولية كلية الحقوق والعلوم السياسية، جامعة مولود مغري، تيزي وزو، ص 04.

³ - رقمي (توضيح) خدمة ويكيبيديا ar.m.wikipedia.org تاريخ الزيارة 2023/05/18 الساعة 20:44.

بلحاج خالدية، فرعون محمد

وبالرغم أن الفكرة العامة التي يمكن استخراجها من هاذين التعريفين أن السيادة الرقمية هي السيطرة والهيمنة على المجال الرقمي إلا أنه وردت تعاريف عديدة للسيادة الرقمية ندرج بعضها فيما يلي:

- أ. هي قدرة الدول على التحكم في البنية التحتية الرقمية الخاصة بها وبيانات مواطنيها، حيث أصبحت التقنيات الرقمية ساحة معركة للتنافس العالمي.
 - ب. هي البعد الرقمي للاستقلالية الاستراتيجية، أي القدرة على اتخاذ القرار والتصرف بشكل مستقل بشأن الجوانب الرقمية الأساسية.
 - ج. هي القدرة على التحكم في مصيرك الرقمي، البيانات والأجهزة والبرامج التي تعتمد عليها وتقوم بإنشائها.
- بالإضافة إلى هذه التعاريف هناك من ميز بين نوعين من السيادة الرقمية:

- 1- السيادة الرقمية للشعوب وهي تشير إلى سيطرة الشعوب والأمم على بياناتهم ومصيرهم على نطاق أوسع إلى جانب مفهوم (سيادة الشبكة) فالتكنولوجيا من هذا المنظور تعد أداة حاسمة لتعزيز السيادة الأصلية.
- 2- السيادة الرقمية الشخصية: تشير إلى التحكم في التقنيات باستخدام برامج مجانية مفتوحة المصدر أو أدوات اتصال مشفرة.

ومن منظور آخر هناك من قدم تعريفا مغايرا تماما لهذا المفهوم حيث أقرنها بسلطة الدول على الشركات التكنولوجية الكبرى ومواقع التواصل، مركزين في ذلك على بعض الحوادث المختلفة حيث أقدمت تويتر على حذف تغريدة لرئيس دولة نيجريا وتعليق حسابه 12 ساعة بدواعي مخالفة محتوى التغريدة لسياسات موقع تويتر، ما أدى إلى غضب سياسي كبير تجاهها معتبرين ذلك ضربة لسيادة دولة نيجريا، كما قامت ذات الشركة بإغلاق حساب الرئيس الأمريكي دونالد ترامب بعد سلسلة من التغريدات التي اعتبرت تحريضية¹

وعليه فإنه يمكننا القول أن السيادة الرقمية من هذا المنظور هي قدرة الدول على التحكم في إدارة وتنظيم وظائف عمالقة التكنولوجيا المعاصرة ومواقع التواصل الاجتماعي ومستخدميها الذين يعدون من مواطني هذه،² حيث تعد السلطة الرمزية قانونية وواقعية تشبه باستقلال ذاتي في العالم الرقمي الذي يعيش فيه مواطنوها ويتفاعلون فيه، فالبيانات الشخصية للأفراد تشكل مادة خام لهاته الشركات وقد يساء استخدامها.³

المطلب الثاني: السيادة الرقمية وبعض المصطلحات المشابهة لها.

هناك مصطلحات تشكل مثيلا للسيادة الرقمية أو جزءا من مضمونها مثل الأمن السيبراني، الردع السيبراني والتحول الرقمي.

¹ - موقع (إيلاف)، سيادة الدولة الرقمية Deelaph.com تاريخ الزيارة: 2023/02/06، الساعة 11:23 سا.

² - موقع (إيلاف) السالف الذكر، تاريخ الزيارة: 2023/02/06، الساعة 12:00.

³ - موقع investglass.com مقال السيادة الرقمية السويسرية، 2023/02/04، تاريخ التصفح 2023/11/10 الساعة 19:13 سا.

أولاً: الأمن السيبراني:

يعرف هنري كيسنجر بأن الأمن هو " أية تصرفات يسعى المجتمع عن طريقها إلى حفظ حقه في البقاء".¹

وهو قدرة الأمم على الدفاع عن سيادتها وحقوقها وصيانة استقلالها، ولم يعد الأمن القومي للدول عرضة لتهديدات تقليدية حيث أضحت الأمن السيبراني جزءاً من الأمن القومي للدول، إذ يعبر عن مجموع الإجراءات والتدابير الأمنية للمحافظة على سرية المعلومات وحماية الشبكات ومنع اختراقها، وهو مزيج من العمليات والتقنيات والبرامج من شأنها حماية البيانات والأجهزة، بالتالي فهو يضم الأمن المادي للشبكات والتطبيقات والأجهزة المعلوماتية وكذا الأمن غير المادي المتعلق بحماية البيانات والمعلومات من أي أضرار متعمدة سواء من قبل دول أخرى أو أشخاص ناشطين في المجال الإلكتروني أو حتى شركات حيث أصبح التجسس الرقمي يمثل أكبر خطر وتهديد الأمن القومي للدول في النظام الحديث.

وتشير التقارير إلى زيادة نسب الجريمة الإلكترونية (كاختراق الأنظمة وسرقة المعلومات وتسريبها).

وصل إلى حد اختراق وزارات هامة وتدمير أنظمتها المعلوماتية وهذه كارثة أمنية تهدد الأمن القومي للدول على اختلاف أبعاده (العسكرية، الاقتصادية، الاجتماعية، الثقافية...) ²، حتى أصبح العالم مفتوحاً على حروب أو هجمات سيبرانية في عالم افتراضي أو فضاء إلكتروني محض يصنفها أهل الاختصاص بحسب الأسلوب إلى:

- هجمات وقف الخدمة (DDOS) بسبب كثرة الرسائل والطلبات ما يؤدي إلى تعطيل الموقع الحكومي ووقف الخدمة المقدمة.

- الأبواب الخلفية (BACK DOORS) وهي عبارة عن برامج الهدف منها التجسس على أجهزة الضحايا وجمع المعلومات حولهم.

وبحسب الهدف أو الغاية من هذه الهجمات والذي قد يكون مالي عن طريق الابتزاز أو سياسي لمحاولة الضغط على الدول لتغيير سياساتها أو وسيلة للتنديد بإزاء قرارات أو مواقف الدول أو قد يكون الهدف عسكري من أجل إضعاف الدول وبحسب الأطراف القائمة بالهجمات والتي قد تكون حكومات أو عصابات منظمة أو أشخاص منفردين أو شركات خاصة.

وهكذا أصبحت الأسلحة السيبرانية بالقوة والخطورة ما قد يفتك بدول أو يزعزع استقرارها ونظامها العام، والتاريخ البشري يحتوي على نماذج كثيرة لهذه الحروب ومثال ذلك تعرض بريطانيا لهجوم سيبراني عرف بهجوم (واناكري) (Wannacrypt) أو (Wannacryptor2.0) أو فيروس الغدية والذي بدأ في 12 ماي

¹ - مسيكة محمد، القضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الحلقة، المجلد السابع، العدد الرابع، 2022.

² - مسيكة محمد، المرجع السابق، ص455.

بلحاج خالدية، فرعون محمد

2017 نتج عنه اختراق أكثر من 230000 جهاز حاسوب حول العالم كما عطل حركة المستشفيات البريطانية ناهيك عن 98 دولة أخرى في العالم كانت ضحية لهذا الهجوم مثل روسيا، أوكرانيا، إسبانيا، فرنسا، والهند وعمان وغيرها.¹

كما تعرضت روسيا إلى هجوم سيرياني استهدف تعطيل مهام رقابة الانتخابات الرئاسية في مارس 2018 للتشكيك في نتائج الاقتراع وهو ما أعلن عنه نائب مدير المركز التنسيقي الروسي لمواجعة حوادث الحاسوب (نيكولاي موشوف).²

ولا ننسى - فضيحة التجسس التي عرفت باسم (برنامج بيغاسوس) المتورط فيها الكيان الصهيوني والذي استهدف التجسس على عديد الشخصيات بالعالم.

ثانيا: الردع الإلكتروني

الردع تعني تعني كبح وأوقف اندفاعه، كف وزجر ومنع ويقال عملية رادعة أي عملية تجربها القوات الأمنية لصد هجوم مرتقب³، وهو كل إجراء أو تصرف يؤدي إلى إقناع طرف إلى الكف عن اتيان سلوك ما، وقد يكون تهديدا أو تشريعا أو قرارا أو غيرها.

أما في الشؤون السياسية الدولية فيعرفه الجنرال "أندريه بوفر"⁴ بأنه: "منع دولة معادية من اتخاذ قرار باستخدام أسلحتها أو بصورة أعم منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديدا كافيا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية⁵."

وتعد نظرية الردع "Deterrence theory" استراتيجية عسكرية ظهرت خلال الحرب الباردة ويستخدم هذا المصطلح للإشارة إلى الاستراتيجية المحتملة لإلحاق ضرر للمعتدي مع التأكيد له بإمكانية تجنب هذا الضرر أو دفعه⁶.

ويرتكز الردع السيرياني على ثلاث دعائم هي⁷:

- ¹ - خدمة ويكيبيديا <https://ar.m.wikipedia.org> هجوم واناكراي الإلكتروني، تاريخ الزيارة 2023/04/28 الساعة 16:06 سا.
- ² - معزي لبند، دهقاني أيوب، الثورة الرقمية في المجال العسكري وتدابيرها على الحروب الحديثة (الحرب السيريانية نموذجاً)، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 07، العدد1، 2022، ص9.
- ³ - تريغف شرح ومعنى "ردع" موقع المعاني <https://almaany.com.ar.ar> تاريخ الزيارة: 2023/04/30 الساعة 09:39 سا.
- ⁴ - أندريه بوفر: André beaufre جنرال فرنسي (1902- 1975) شارك في الحرب العالمية الثانية وكذا العدوان الثلاثي على مصر.
- ⁵ - علاء الدين فرحات، من الردع النووي إلى الردع السيرياني دراسة لمدى تحقيق مبدأ الردع في القضاء السيرياني مجلة المفكر، المجلد 16/ العدد 01، 2021، ص271.
- ⁶ - نظرية الردع، موقع المعرفة m.marefa.org تاريخ الزيارة: 2023/04/30 الساعة: 22:12 سا.
- ⁷ - الردع السيرياني، المفهوم والإشكاليات والمتطلبات، موقع <https://de.moratica.de> تاريخ الزيارة: 2023/04/30 على الساعة: 22:55 سا.

السيادة الرقمية

أ- **مصادقية الردع:** حيث يتطلب الدفاع عن الأنظمة المعلوماتية توفر أنظمة نسخ احتياطية ما يحبط التدمير التام للأنظمة أو فقدانها كلية ويعد ذلك حلا عمليا وأكثر فاعلية.

ب- **القدرة على الانتقام:** حيث بعد التعرف على المهاجم السيرياني يجب أن يمتاز بالقدرة على رد الهجوم وتكبيد المهاجم ضررا يفوق ما خلفه هجومه.

ت- **الرغبة في الانتقام:** حيث أن امتلاك القدرة على الانتقام من المهاجم السيرياني غير كافية بل يجب أن يصاحب ذلك إعلان صريح من المدافع برغبته في الانتقام.

كما ميز الكتاب أن نميز بين عنصرين أساسيين للردع السيرياني وهما¹ :

1- **الردع بالمنع:** ويكون فعالا عند إقناع بعدم تحقيق أرباح لدى المهاجم حيث أن تكلفة الهجوم تفوق مكاسبه وذلك بسبب الأنظمة الدفاعية التي تحول دون نجاح أي هجوم².

2- **الردع بالعقاب:** وينطوي تحت هذا العنصر — الردع بالمقاومة (Résistance) والردع بالصمود (Résilience) والهدف منها تقليل الخيارات أمام المفكر في الهجوم وذلك من خلال بناء هيكل دفاعية يصعب التغلب عليها أو ضمان الاستعادة السريعة لأصل الشيء بعد الهجوم .

ثالثا: التحول الرقمي:

بات التحول الرقمي خيارا استراتيجيا في ظل التطور التكنولوجي الهائل الذي عرفه العالم، حيث اكتسح جميع مجالات الحياة، لذلك وردت تعريف عديدة له بحسب مجال تخصصه.

فاقتصاديا هو عملية شاملة ناتجة عن مزيج من ثلاث ظواهر: الأتمتة (automation) إزالة الطابع المادي وإعادة تنظيم أنماط الوساطة.³

والأتمتة هي استخدام أجهزة الكمبيوتر والمعالجات والبرمجيات في مختلف الميادين والقطاعات سواء الخدمية أو التجارية أو الصناعية أو المصرفية لغرض السير الجيد والفعال بأقل خطأ ممكن⁴، وهي التنفيذ الآلي لقواعد العمل والمهام الوظائف من خلال أجهزة أوتوماتيكية مبرمجة لذلك.

¹ - علاء الدين فرحات، المرجع السابق، ص 273.

² - عبد الغفار الديواني، الردع الإلكتروني بين المنع والانتقام، مركز المستقبل futureuae.com، تاريخ الزيارة: 2024/04/30 الساعة: 23:11 سا.

³ - نقاوة رانية، شوام بوشامة، التحول الرقمي خيار استراتيجي في ظل الانتقال نحو الاقتصاد الرقمي في الجزائر، دراسة استكشافية، مجلة الاقتصاد والبيئة، المجلد 06، العدد 01 أبريل 2023، ص 422.

⁴ - صدوقي غريسي، سي الطيب الهشي رضا، علي العبيسي، واقع وأهمية التحول الرقمي والأتمتة، مجلة آراء للدراسات الاقتصادية والإدارية، ص 104.

بلحاج خالدية، فرعون محمد

ويقصد بإزالة الطابع المادي: التجريد من خلال اكتشاف قنوات جديدة للاتصال والتوزيع والتخلي عن سابقتها التقليدية المادية والتقليل من التكاليف.

أما إعادة تنظيم أنماط الوساطة فهي بغرض تحديد أدوار الفاعلين تبني نماذج أعمال جديدة تعتمد على التقنيات التكنولوجية¹، مرتكزا على المعطيات والبيانات واستخدامها على شكل خوارزميات معقدة وسلاسل برمجية تؤدي إلى تنفيذ الوظائف والمهام المتورطة بها، حيث يشير مصطلح التحول الرقمي إلى الآثار الاقتصادية والاجتماعية للرقمنة وهي تحويل البيانات والعمليات التناظرية إلى تنسيق يمكن للآلية قراءته، وكذا الرقمنة ويقصد بها ترابط البيانات الرقمية والتقنيات لإحداث تغييرات جديدة في الأنشطة الحالية.²

وعليه فإن عملية التحول الرقمي تستلزم دعما من الإدارة المركزية (العليا) كفاءة الموارد البشرية خبرة واسعة في مجال الحاسب الآلي وتدريب عملي على البرامج والتطبيقات بالإضافة إلى ضرورة توفر الأجهزة الإلكترونية والوسائل التقنية.

وتظهر جليا الفوائد الجمّة للتحول الرقمي وذلك من خلال:

- تحسين جودة المنتجات والخدمات المقدمة
- تسهيل الوظائف والأعمال.
- تحسين الكفاءة والتقليل من الأخطاء المركزية.
- التقليل من التكاليف.
- الحد من البيروقراطية.
- رفع مستوى الشفافية بين الإدارة والمواطن.

المبحث الثاني: آليات حماية السيادة الرقمية.

انتهج الدول آليات قصد حماية سيادتها الرقمية ولكن قبل التطرق إلى جهودها في هذا المجال كان لزاما البحث في صور الاعتداءات الذي قد تتعرض لها السيادة الرقمية.

أولا: صور الاعتداء على السيادة الرقمية.

هناك صور عديدة تشكل مساسا بالسيادة الرقمية غير أنه يمكن تقسيمها أو تصنيفها ضمن إطارين أساسيتين هما المساس بسرية المعلومات والبيانات والمساس بسلامة الأنظمة والأجهزة المعلوماتية.

¹ - صدوقي غريسي، سي الطيب الهشي رضا، علي العبيسي، المرجع نفسه، ص102.

² - لعرج مجاهد نسمة، مجلة دفاتر MECAS مجلد 17، العدد 04، ديسمبر 2021، ص343.

السيادة الرقمية

أ. المساس بسرية وسلامة المعلومات.

تنطوي تحت هذا العنوان عديد الأساليب والسلوكات التي تمس بسرية وسلامة المعلومات والبيانات، حيث يشمل الدخول غير المشروع الاعتراض غير المشروع والتلاعب بالبيانات والمعطيات.

أولاً: الدخول غير المشروع:

نصت عليه اتفاقية بودابست عن عنوان الدخول غير القانوني وجرمته المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات¹، وهو قيام دولة أو جهاز أو فرد بالاطلاع على بيانات سرية غير متاحة لعامة الناس تكون محفوظة على أنظمة معلوماتية أو شبكات الاتصال بواسطة عمليات وتقنيات سرية وذرائع مزيفة بدون ترخيص من مستخدمي هذه الأنظمة.²

ويتحقق هذا الاعتداء عن طريق الدخول غير المشروع أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات سواء تعلق بالحكومة الإلكترونية أو أي نظام إلكتروني آخر، ويعد الدخول مشروعاً متى كان سهلاً أو حتى مصادفة أو عن طريق الخطأ، وفي حال البقاء يعد ذلك تعمداً ومنه يتوفر لديه قصداً جنائياً يعاقب عليه حسب القوانين الوطنية.³

ثانياً: الاعتراض غير المشروع:

وهو ما يطلق عليه أيضاً التجسس الإلكتروني أو الاعتراض غير القانوني للبيانات ويعد وسيلة لجمع المعلومات بطريقة إلكترونية عن طريق الولوج إلى الحسابات والمواقع والمنصات الرقمية الحكومية والخاصة وتحليل هذه المعلومات والبيانات ما قد يكشف تفاصيل عديدة غير مرغوب فيها ويجعلها عرضة لسوء الاستخدام والاستغلال كالقيام ببيع هذه المعلومات لجهات معادية.

واعترض نظام المعلوماتية معروف في الولايات المتحدة الأمريكية باسم (Electromagnetic pickup) التقاط الموجات الكهربية وهو جمع المعلومات عن بعد لذلك يعتقد أن الوسيلة الأساسية لاعتراض أنظمة المعلوماتية هي استخدام الموجات الكهربية الصادرة عن النظام. (Electromagnetic Radiation)⁴

¹ - شعيرط أحمد، قريز مراد، تحديات الانترنت لسيادة الدولة (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، مجلد 5، العدد 01، 2022، ص 305.

² - ربيعي حسين، سمر محمود، الحروب السيبرانية الخطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلد 07، العدد 02، ص 182.

³ - عبد الفتاح بيومي مجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، مصر، المجلة الكبرى، 2008، ص 361.

⁴ - عباوي نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاثر السياسة والقانون، العدد 16، جانفي 2017، 285.

ثالثاً: التلاعب بالبيانات والمعطيات:

يكون عن طريق الإدخال، المحو، والتعديل، ما يعد مساساً بسلامة البيانات ويقصد "بفعل الإدخال" إضافة معطيات جديدة على الدعامة الإلكترونية سواء كانت خالية أو محتواة على معطيات من قبل، وغالباً ما ترتكب هذه الجريمة من قبل شخص مؤهل لارتكاب هذا التلاعب كأن يكون مسؤولاً أو موظفاً في القسم المعلوماتي.¹

وبما أن التقنية الحديثة اكتسحت تقريباً كل نواحي الحياة العملية، الاقتصادية والاجتماعية وغيرها، جعل حالات التلاعب بالمعطيات لا حصر لها وإن كانت تتفاوت فيما بينها من حيث قيمة الخسائر وعدد الجرائم المرتكبة ما يدفعنا إلى القول أن المجال المالي من أبرز الميادين التي تنتشر فيها جريمة التلاعب بالبيانات خاصة التلاعب بأنظمة التحويل الآلي للأموال والتلاعب باستعمال بطاقة الائتمان المغنطة.²

ب. المساس بسلامة الأجهزة والأنظمة المعلوماتية:

ويمكن أن ندرج تحت هذا البند كلا من المساس بسلامة النظام وسوء استعمال الأجهزة المعلوماتية.

1- المساس بسلامة النظام:

ويقصد بالنظام المكونات المادية والمنطقية للشبكة، حيث تضم المكونات المادية كافة المعدات المستخدمة في تشغيله كالأسطوانات والكابلات والحواشيب... إلخ، والتي قد تكون عرضة للسرقة، الاتلاف والحرق العمديين وغيرها.

أما المكونات المنطقية فهي تضم البرامج والتطبيقات وأنظمة الاستغلال وكذا قواعد البيانات وهي بدورها قد تكون معرضة للإتلاف والتخريب من خلال زرع البرامج الضارة والفيروسات ما يؤدي إلى إيقاف تشغيل نظام الشبكات والاتصالات وعرقلة وصول المعلومات أو التأثير على كفاءة عملها وتغيير مسارها³، ومثال ذلك فيروس

2- سوء استعمال الأجهزة المعلوماتية:

وتمثل في تقديم أو إنتاج برامج أو توزيع أجهزة معلوماتية لأغراض سيئة وتدخل ضمنها أيضاً بيع كلمات الأسرار والبيانات للأشخاص دون وجه حق ما يسهل اختراق المواقع والحاسبات الخاصة وبالتالي انتهاك

¹ - عبد الفتاح بيومي حجازي، المرجع السابق، ص 364.

² - عباوي نجاة، المرجع السابق، ص 287.

³ - المرجع السابق، ص 206.

السيادة الرقمية

خصوصية الأشخاص وبياناتهم الرقمية سواء أجريت المعالجة الإلكترونية بواسطة شخص خاص أو عام¹، فهو ما قد يؤدي إلى تلف البيانات وضيعاها.

المطلب الثاني: حماية السيادة الرقمية

اعترافا ضمنيا بحساسية موضوع السيادة الرقمية وأهميته البالغة، سعت دول العالم إلى تكريس الحماية لسيادتها الرقمية وذلك بانتهاج أساليب وآليات مختلفة سواء في الشق القانوني أو التشريعي أو في شقها التنظيمي من خلال إنشاء هيئات وأجهزة توكل لها مهام الحماية والحفاظ على السيادة الرقمية للدول من أي انتهاك.

أولا: الآليات القانونية:

مما لا شك فيه أن مواجهة أي انتهاك للسيادة الرقمية للدول يستوجب نظاما قانونيا يضمن شرعية المكافحة من خلال توفير الركن الشرعي المحترم للسلوك لذا دأبت الدول والحكومات سواء في شكل تكتلات أو من خلال المنظمات أو حتى بشكل انفرادي إلى سن قواعد وباعتبار الجرائم الماسة بالسيادة الرقمية للدول عابرة للحدود يستلزم تعاون دوليا وردود فعل سريعة في إطار قانوني، ففي الجزائر تم تعديل قانون العقوبات بما يتلاءم والتطور التكنولوجي وكذا الإجرامي وذلك بموجب القانون 10/04 المؤرخ في 10/11/2004 حيث تضمن قسم خاص بالمساحات بأنظمة المعالجة الآلية للمعطيات، حيث جزم الولوج والبقاء عن طريق الغش في منظومة للمعالجة الآلية للمعطيات وإحداث أي تغيير فيها أو تخريب نظام تشغيلها أو إزالتها أو تعديلها أو استعمالها مشددا العقوبة إذا استهدفت الجريمة هيئات حساسة في البلاد كالإدارة الوطنية ومعاقبا على الشروع فيها أيضا بنفس العقوبة لارتكابها.

وكذا قانون الإجراءات الجزائية حيث تم تحديد الاختصاص المحلي لوكيل الجمهورية في الجرائم المعلوماتية، ناهيك عن القانون 04/09 المؤرخ في 05/08/2009 والمتضمن لقواعد الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

أما في دولة ليبيا فقد تم إصدار القانون رقم 5 لسنة 2022 المتعلق بمكافحة الجرائم الإلكترونية حيث تضمنت المادة الأولى منه تعريفا لبعض المفاهيم كالجريمة الإلكترونية، القرصنة الإلكترونية، الفيروسات الحاسوبية، إعاقة الوصول إلى الخدمة، الالتقاط أو الاعتراض، ومبرزا أهداف القانون والتي من بينها الحد من الجرائم الإلكترونية، وتحقيق الأمن المعلوماتي وحماية الاقتصاد الوطني، مجرما الدخول غير المشروع، الاعتراض أو التعرض، التعدي على نظام معلوماتي للحصول على منفعة مادية، التغذي على نظام معلوماتي واستخدام معطياته، تعطيل الأعمال الحكومية، إتلاف الأدلة القضائية الرقمية، التنصت غير المشروع².

¹ - الآليات القانونية المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، المجلد 07، العدد 02،

2022، ص 195

² - موقع المجتمع القانوني الليبي <https://lowsociety.ly.legislation> تاريخ الزيارة: 06/06/2024 الساعة 19:15.

بلحاج خالدية، فرعون محمد

والصين باعتبارها قوة سبانية صاعدة، وأكبت سياستها التشريعية التطورات والتحولات في المجال الرقمي فبداية من تشريع لجنة إدارة التشفير في سنة 1999 والذي كان يهدف إلى ضرورة تمرير كافة المنتجات الأجنبية والتكنولوجية منها إلى هذه اللجنة، إلى تشريع "السد الأخضر- مرافقة الشباب" (Green dam – youth escort) في ماي 2009 وهو عبارة عن برنامج لتصفية الواب صادر عن وزارة الصناعة وتكنولوجيا المعلومات الصينية (MIIT) والذي قوبل باحتجاجات كبيرة خاصة من الولايات المتحدة الأمريكية حيث اعتبر تقييدا لحرية التعبير والحرية الشخصية وصولا إلى إصدار قانون الأمن السباني الصيني في 2014 وهو القانون الذي فرض على شركات التكنولوجيا المزودة للبنوك الصينية بالبرامج والأجهزة بمشاركة كود المصدر الخاص بها كدليل على عدم استخدام التكنولوجيا كغطاء لأغراض تجسسية.¹

أما الاتحاد الأوروبي فقد أقر لائحة تنظيمية وقانونا أوروبا لحماية البيانات سمي "اللائحة العامة لحماية البيانات (GDPR)" General data protection regulation يهدف إلى حماية البيانات الخاصة بالمواطنين الأوروبيين حيث يركز على سبعة مبادئ أساسية مرتبطة بالبيانات الشخصية من بينها المشروعية القانونية، الدقة، قيود التخزين، النزاهة، السرية، الأمان، وتحمل المسؤولية.

وقد تم اعتماد هذا النظام في 2026/04/14 ليصبح نافذا في 2018/05/25²

ونعرض فيما يلي مقارنة لأهم الآليات القانونية ببعض عمالققة التكنولوجيا على النحو المبين بالجدول:³

الدولة	قانون حماية البيانات الشخصية	الهيئة المكلفة بالرقابة	الغاية المرجوة
الصين PRC	قانون حماية المعلومات الشخصية PIPL	الإدارة الوطنية لحماية البيانات NPA	تهدف إلى ضمان الاستقرار السياسي من خلال سيطرتها على البيانات الشخصية، ومراقبة المواطنين خوفا من استخدام بياناتهم في أغراض تمس بالنظام الحالي
الاتحاد الأوروبي EU	اللائحة العامة لحماية البيانات GDPR	اللجنة الأوروبية لحماية البيانات EDPB	تهدف إلى حماية حقوق المواطنين الأوروبيين وتعزيز الخصوصية الرقمية بعيدا عن استغلال الشركات التكنولوجية الكبرى
و.م.أ USA	لا يوجد قانون وطني لحماية البيانات ولكن هناك قوانين ولاية عديدة منها: قانون المستهلك بكاليفورنيا الذي يسمح بتبادل المعلومات الشخصية CCPA وقانون إخضاع نقل التأمين الصحي والمسؤولية HIAAA	اللجنة الفيدرالية للتجارة	تركز على الحقوق الفردية وكذا حرية الشركات وعدم في جرائم الابتزاز الرقمي والتجسس التجاري بضمان حماية المعلومات

¹ - خرماسة عبدالرحمن، مخبر الدراسات القانونية البيئية، جامعة 08 ماي 1945 قالمة، السياسة الرقمية الصينية، قراءة في التشريعات الوطنية لتأمين السيادة الرقمية. The chinese digital policy ; Areading of ,ational legislation for ensuring digital. السيادة الرقمية للدولة، سياسات وتجارب مقارنة، عدد خاص، ص 07.

² - خدمة ويكيبيديا: النظام الأوروبي العام لحماية البيانات ar.m.wikipedia.org تاريخ التصفح: 2024/06/07 الساعة 18:49.

³ - خرماسة عبد الرحمان، المرجع السابق، ص 07.

السيادة الرقمية

وعلى صعيد آخر واضطلاعا بدورها كفرد من المجتمع الدولي حذت المنظمات الدولية حذو الدول في سعيها لإيجاد آليات مناسبة للتصدي للأُنشطة الماسة بالسيادة الرقمية للدول المنضوية تحت لوائها وذلك من خلال عقد عدة مؤتمرات لمناقشة هذا الموضوع الحساس والخروج باتفاقيات ملزمة، وعلى رأس هذه المنظمات هيئة الأمم المتحدة التي منذ سنة 1990 تاريخ انعقاد مؤتمرها الثامن بهافانا (كوبا) المخصص لمنع الجريمة وتبادل المساعدة في المسائل الجنائية الذي طالب بحماية مصالح وحقوق ضحايا جرائم الحاسوب إلى مؤتمرها التاسع بالقاهرة في 1995، حيث أوصت بضرورة حماية الفرد من مخاطر التكنولوجيا، إلى المؤتمر بضرورة حماية الفرد من مخاطر التكنولوجيا، إلى المؤتمر الثاني عشر- في 2010 والذي انعقد بسالفادور (البرازيل) أين تم مناقشة الجرائم الإلكترونية بتعمق أكبر، حيث جاء البند الواحد والأربعون والثاني والأربعون من تقريره تأكيدا على ذلك، وصولا إلى مؤتمرها الثالث عشر- المنعقد في مدينة الدوحة بقطر والذي فرج بعدة توصيات في مجال مكافحة الجرائم السيبرانية من بينها وجوب استحداث آليات لمكافحتها بالاعتماد على استراتيجيات جديدة مع إشراك القطاع الخاص، وبالإضافة إلى هذه المؤتمرات أصدرت الهيئة دليلا حول جرائم المعلوماتية يتم تعديله مواءمة لأي جديد.¹

ثانيا : الآليات التنظيمية أو الهيكلية

لا تكتمل الجهود القانونية إلا بوجود أجهزة وهيئات تسهر على التطبيق الفعلي للقواعد القانونية على أرض الواقع، فعلى المستوى الوطني تم إنشاء عديد الأجهزة المختصة في مكافحة الجرائم ذات الطابع الرقمي والتي من شأنها تهديد السيادة الرقمية للدولة الجزائرية وتسجل في هذا المقام إنشاء خلية لمحاربة الجريمة الإلكترونية على مستوى المديرية العامة للأمن الوطني (DGSN) سنة 2011 لتيتم فيما بعد إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال التابعة لمديرية الشرطة القضائية وذلك في سنة 2015 والتي تعد مصلحة عملياتية نشطة متخصصة تضم محققين ذو كفاءة عالية في مجال التفتيش الإلكتروني حيث تم إحصاء 323 قضية سنة 2022 و 331 قضية في سنة 2023 تمس بأنظمة المعالجة الآلية للمعطيات.²

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي وجرائم المعلوماتية للدرك الوطني في 2008 ويأتي هذا في إطار استراتيجية الجيش الوطني الشعبي في الدفاع عن السيادة الرقمية للدولة الجزائرية وتحقيق نظام متكامل يغطي كافة الجوانب سواء الوقائية منها أو للكشف والرد على أي هجمات سيبرانية مع مواكبة التطور التقني السريع في العالم في ظل تعاون دولي مع الدول الصديقة للاستفادة من خبراتهم في هذا المجال.³

¹ - بيدي أمال، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، سنة 2022، ص 309.

² - مجلة الشرطة، مجلة أمنية إعلامية، تصدر عن المديرية العامة للأمن الوطني، العدد 158 ماي 2024، ص 21.

³ - شعيرط أحمد، قريزيمراد، تحديات الانترنت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 01، 2022،

بلحاج خالدية، فرعون محمد

ولنفس الأهداف تم بموجب المرسوم الرئاسي 05/20 إنشاء المجلس الوطني لأمن الأنظمة المعلوماتية برئاسة وزير الدفاع الوطني أو ممثل عنه، له مهام إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، كما يضم وكالة لأمن الأنظمة المعلوماتية والتي تعد وفقا للمادة 17 من المرسوم الرئاسي المذكور أنفا مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية تقوم بالتنسيق وتنفي الخطة الوطنية في مجال تأمين الأنظمة المعلوماتية وإجراء التحقيقات في حالة الهجمات السيبرانية المستهدفة للمؤسسات الوطنية وجمع وتحليل المعطيات والبيانات ذات الصلة.¹

وبموجب المرسوم الرئاسي 261/15 الصادر في 2015/11/08 تم تشكيل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وهي هيئة إدارية مستقلة تتمتع أيضا بالشخصية المعنوية مقرها الجزائر العاصمة، وتوضع لدى وزير العدل وتعمل تحت رقابة السلطة القضائية حيث تقوم بتنسيق عمليات الوقاية ومساعدة الجهات القضائية من خلال جمع المعلومات وضمان المراقبة وتسجيل وحفظ المعطيات الرقمية وتحديد مسارها لاستخدامها في مجال الإجراءات القضائية.²

ولا تقتصر جهود الجزائر لحماية سيادتها الرقمية على هذا فحسب بل هناك مشاريع وتطلعات أكبر مثل إنجاز المركز الوطني الجزائري للخدمات الرقمية والذي من شأنه أن يكون خطوة عملاقة باتجاه تحقيق الاستقلال التكنولوجي وتعزيز البنى التحتية في المجال الرقمي والذي سوف ينجز على مراحل بالتعاون مع مجتمع "هواوي كونسورسيوم".³

أما على الصعيد الدولي ویرغم التطور الذي تعرفه دول الاتحاد الأوروبي إلا أنها لا تزال تابعة في بعض منها إلى العملاقين الولايات المتحدة الأمريكية والصين المتنافسين على الريادة، وهذا ما يجعلها تسعى إلى البحث على اعتماد استراتيجية قصد تحقيق استقلالها التكنولوجي التام مثل فرنسا التي أعلنت عن توقف بعض هيئاتها الرسمية على استعمال محرك البحث غوغل (GOOGLE) واستبداله بمحرك البحث كوانت (QWANT) وهو محرك بحث تم إطلاقه في فبراير 2013 يركز على الخصوصية ويدعي أنه لا يتتبع المستخدمين أو يعيد بيع بياناتهم الشخصية.⁴

كما أنشأت في سنة 2009 الوكالة الوطنية لأمن أنظمة المعلومات (ANSSI).⁵

¹ - حزام فتية، حاية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية، قراءة في أحكام المرسوم الرئاسي 05/20، مجلة الحقوق والعلوم الإنسانية، العدد 03، أكتوبر 2020، ص 182-183.

² - حلم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاثر البحوث العلمية، المجلد 09، العدد 01، 2021، ص 228.

³ - المركز الوطني الجزائري للخدمات الرقمية، خطوة نحو تعزيز السيادة الرقمية لتحقيقا للاستقلال التكنولوجي، وكالة الأنباء الجزائرية APS.dz تاريخ النسخ 2024/06/08 الساعة 08:07.

⁴ - موقع الجزيرة نت www.aljazeera.net.cdn.ampproject فرنسا تستخدم كوانت بدل غوغل لاستعادة سيادتها الرقمية، تاريخ الزيارة 2024/03/28 الساعة 23:03.

⁵ - شعريط أحمد، قريبيز مراد، المرجع السابق، ص 314.

السيادة الرقمية

وعلى المستوى دول الجوار كانت تونس سباقة في إنشاء الوكالة الوطنية للسلامة المعلوماتية سنة 2014 ومنذ 2019 بدأت في تنظيم ورشات عمل تهتم بحماية البنية التحتية الرقمية الحيوية استجابة لأبي طارئ.¹

وعلى غرار الدول أنشأت المنظمات الدولية أجهزتها لحماية السيادة الرقمية لدولها، كالاتحاد الدولي للاتصالات الذي يلعب دورا كبيرا في الاتصالات ومسائل الأمن المعلوماتي من خلال الدعوة إلى قمتين عالميتين حول المعلوماتية ولتيم إطلاق ما سمي بالبرنامج العالمي للأمن المعلوماتي للاتحاد الدولي للاتصالات الذي يركز على بناء القدرات قصد تعزيز الأمن السيبراني.²

خاتمة:

كما يقال كل ابتكار لا يخلو من العيوب، والتكنولوجيا على قدر الفائدة التي قدمتها للبشرية في تسهيل الأمور الحياتية، إلا أنها سلاح ذو حدين، حيث جردت الدول من خصوصيتها وجعلت بعض أسرارها عرضة للكشف ومواطنيها عرضة للابتزاز والمتاجرة ببناتهم الشخصية، ناهيك عن منصات التواصل الاجتماعي التي يحق لها نشر ما تريد وفق سياستها الخاصة دون النظر إلى سياسات الدول وتوجهاتها، وعليه وجب على جميع الدول دعم بنائها التكنولوجية التحتية وإيجاد مقومات البقاء كتكوين المورد البشري في المجال الإلكتروني وتوعيته تجاه حساسية التواجد في العالم الافتراضي في زمن إجبارية الرقمنة بالإضافة إلى استيراد التكنولوجيات الحديثة للدفاع عن سيادتها.

قائمة المراجع:

1. الردع السيبراني، المفهوم والإشكاليات والمتطلبات، موقع <https://de.moratica.de> تاريخ الزيارة: 2023/04/30 على الساعة: 22:55 سا.
2. المركز الوطني الجزائري للخدمات الرقمية، خطوة نحو تعزيز السيادة الرقمية تحقيقا للاستقلال التكنولوجي، وكالة الأنباء الجزائرية APS.dz تاريخ التصفح 2024/06/08 الساعة 08:07.
3. أندريه بوفر: André beaufre جنرال فرنسي- (1902- 1975) شارك في الحرب العالمية الثانية وكذا العدوان الثلاثي على مصر.
4. بيدي أمال، جهود الأمم المتحدة في مكافحة الجريمة السيبرانية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد 08، العدد 01، سنة 2022.
5. تعريف شرح ومعنى "ردع" موقع المعاني <https://almaany.com.ar.ar> تاريخ الزيارة: 2023/04/30 الساعة 09:39 سا.

¹ - حزام فتيحة، المرجع السابق، ص 182.

² - شعريط أحمد، قرييز مراد، المرجع السابق، ص 316.

بلحاح خالدية، فرعون محمد

6. تفاؤلية، شوام بوشامة، التحول الرقمي كخيار استراتيجي في ظل الانتقال نحو الاقتصاد الرقمي في الجزائر، دراسة استكشافية، مجلة الاقتصاد والبيئة، المجلد 06، العدد 01 أبريل 2023.
7. حزام فتية، حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية، قراءة في أحكام المرسوم الرئاسي 05/20، مجلة الحقوق والعلوم الإنسانية، العدد 03، أكتوبر 2020.
8. حلبي رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاير البحوث العلمية، المجلد 09، العدد 01، 2021.
9. حمير سمير، محاضرات حول إشكالية مفهوم السيادة الوطنية في ظل المتغيرات الدولية الراهنة، قسم العلوم السياسية والعلاقات الدولية كلية الحقوق والعلوم السياسية، جامعة مولود معري، تيزي وزو.
10. خدمة ويكيبيديا: النظام الأوروبي العام لحماية البيانات ar.m.wikipedia.org تاريخ التصفح: 2024/06/07 الساعة 18:49.
11. خرمازة عبدالرحمن، مخبر الدراسات القانونية البيئية، جامعة 08 ماي 1945 قالمة، السياسة الرقمية الصينية، قراءة في التشريعات الوطنية لتأمين السيادة الرقمية. *The chinese digital policy ; Areading of*, ational. *legislation for ensuring digital* السيادة الرقمية للدولة، سياسات وتجارب مقارنة، عدد خاص.
12. ربيعي حسين، سمر محمود، الحروب السيبرانية الخطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي، المجلد 07، العدد 02.
13. رقمي (توضيح) خدمة ويكيبيديا ar.m.wikipidia.org تاريخ الزيارة 2023/05/18 الساعة 20:44.
14. شحيرط أحمد، قريبيز مراد، تحديات الانترنت لسيادة الدولة (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، مجلد 5، العدد 01، 2022.
15. صدوقي غريسي، سي الطيب الهشمي رضا، علي العبسي، واقع وأهمية التحول الرقمي والأتمتة، مجلة آراء للدراسات الاقتصادية والإدارية.
16. عباوي نجاة، الإشكالات القانونية في تجريم الاعتداء على أنظمة المعلومات، دفاير السياسة والقانون، العدد 16، جانفي 2017.
17. عبد الغفار الديواني، الردع الإلكتروني بين المنع والانتقام، مركز المستقبل futureuae.com تاريخ الزيارة: 2024/04/30 الساعة 23:11 سا.
18. عبد الفتاح بيومي مجازي، النظام القانوني للحكومة الإلكترونية، الكتاب الثاني الحماية الجنائية والمعلوماتية للحكومة الإلكترونية، دار الكتب القانونية، مصر، المجلد الكبير، 2008.
19. علاء الدين فرحات، من الردع النووي إلى الردع السيبراني دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني مجلة المفكر، المجلد 16 / العدد 01، 2021.
20. لعرج مجاهد نسيم، مجلة دفاير MECAS مجلد 17، العدد 04، ديسمبر 2021.
21. مجلة الشرطة، مجلة أمنية إعلامية، تصدر عن المديرية العامة للأمن الوطني، العدد 158 ماي 2024.

السيادة الرقمية

22. مسيكة محمد، القضاء السيبراني وتحديات الأمن القومي للدول، مجلة العلوم القانونية والاجتماعية، جامعة زيان عاشور، الجلفة، المجلد السابع، العدد الرابع، 2022.
23. موقع (إيلاف) السالف الذكر ، تاريخ الزيارة: 2023/02/06، الساعة 12:00.
24. موقع (إيلاف)، سيادة الدولة الرقمية Deelaph.com تاريخ الزيارة: 2023/02/06، الساعة 11:23 سا.
25. موقع investglass.com مقال السيادة الرقمية السويدية، 2023/02/04، تاريخ التصفح 2023/11/10 الساعة 19:13 سا.
26. موقع الجزيرة نت www.aljazeera.nt.cdn.ampproject فرنسا تستخدم كوانت بدل غوغل لاستعادة سيادتها الرقمية، تاريخ الزيارة 2024/03/28 الساعة 23:03.
27. موقع المجتمع القانوني الليبي <https://lowsociety.ly.legislation> تاريخ الزيارة: 2024/06/06 الساعة 19:15.
28. موقع المعالي <https://www.almaany.com.ar.ar> تعريف السيادة في معجم المعاني الجامع، معجم عربي عربي، تاريخ الزيارة 2023/02/17 الساعة 18:54 سا.
29. نظرية الردع، موقع المعرفة m.marefa.org تاريخ الزيارة: 2023/04/30 الساعة 22:12 سا.
30. خدمة ويكيبيديا <https://ar.m.wikipedia.org> هجوم واناكراي الإلكتروني، تاريخ الزيارة 2023/04/28 الساعة 16:06 سا.
31. شخريط أحمد، قرييز مراد، تحديات الانترنت لسيادة الدول (السيادة الرقمية)، مجلة البحوث القانونية والاقتصادية، المجلد 05، العدد 01، 2022.
32. معيزي ليندة، دهقاني أيوب، الثورة الرقمية في المجال العسكري وتدابيرها على الحروب الحديثة (الحرب السيبرانية نموذجاً)، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 07، العدد 1، 2022.