دور حوكمة إدارة البيانات في مكافحة الجريمة السبيرانية وتعزيز السيادة الرقمية.

The role of data governance in combating cybercrime and promoting digital sovereignty

عبد المالك تلي

جامعة ورقلة، الجزائر، telli.abdelmalek@univ-ouargla.dz

فريدة طاجين

جامعة ورقلة، الجزائر، tadjine.farida@univ-ouargla.dz

تاريخ الإرسال:2026/04/27 * تاريخ القبول2026/05/31* تاريخ النشر: 02/ 06 /2026

ملخص: تتناول هذه الدراسة دور حوكمة إدارة البيانات كإطار لمكافحة الجريمة السبيرانية وتعزيز السيادة الرقمية للدول في ظل تسارع التحول الرقمي للمجتمعات والدول ، والذي أفرز تحديات أمنية أكثر تعقيدا وتشابكا، وينطلق البحث من أن تزايد وتيرة وحدّة الجرائم السيبرانية العابرة للحدود الوطنية تجاوز تهديد أمن الأفراد والمؤسسات إلى أمن البيانات الوطنية والسيادة الرقمية للدول مما يهدد أمنها القومي، وتم طرح تساؤلات عن كيفية مساهمة حوكمة البيانات في تقليل مخاطر الجريمة السيبرانية وتقوية السيادة الرقمية بهدف تفكيك العناصر المفهوماتية الأساسية، وتحليل طبيعة التفاعل فيما بينها، و إبراز فعالية حوكمة البيانات في دعم التحكم السيادي في الموارد الرقمية ،واعتمد البحث على المنهج الوصفي التحليلي بتحليل مختلف الأدبيات والوثائق العلمية والتنظيمية والسياسية للمفاهيم وتحليل أبعادها القانونية والمؤسساتية والتقنية، والأدوار الحقيقية لإدارة البيانات في مكافحة الجريمة السيبرانية وتعزيز السيادة الرقمية في بعض التجارب الدولية،وخلص البحث إلى أن حوكمة إدارة البيانات هي أحد أهم الأدوات وأنجع طرق تعزيز الأمن السيبراني والسيادة الرقمية ،كونها تمكن الدول من تنظيم تدفق البيانات وحمايتها من الاستغلال وتقليل التبعية التكنولوجية، غير أن نجاح الدول في ذلك يعتمد بشكل كلي على مدى قدرتها على صناعة نماذج سيادية رقمية فعالة لإدارة البيانات وتطوير بنيتها التحتية الرقمية وسن تشريعات تواكب التغيرات المتسارعة في الفضاء الرقمي.

الكلمات المفتاحية:الأمن السبيراني، التحول الرقمي، الجريمة السبيرانية، حوكمة إدارة البيانات، السيادة الرقمية.

Abstract: This study examines the role of data governance as a framework for combating cybercrime and enhancing digital sovereignty of states in context of accelerating digital transformation, which has generated increasingly complex and interconnected security challenges. The research assumes that the growing cross-border cybercrime no longer threatens only individuals and institutions, but also undermines national data security, endanger states' digital sovereignty. Accordingly, it raises questions about how data governance can contribute to reducing cybercrime risks and strengthening digital sovereignty, deconstructing the key conceptual foundations of the topic and analyzing the nature of their interrelation ships. It adopts a descriptive-analytical approach, drawing on a review of relevant academic literature, regulatory documents, and public policies, with particular attention to legal, institutional, and technical dimensions, as well as selected international experiences in data management, cybercrime prevention, and digital sovereignty.The findings indicate that data governance constitutes one of the most effective tools for enhancing cybersecurity and digital sovereignty, as it enables states to regulate data flows, protect data from misuse, and reduce technological dependency. However, its effectiveness ultimately depends on states' capacity to develop robust digital sovereignty models, modernize digital infrastructure, and enact adaptive legislation that keeps pace with rapid transformations in cyberspace.

Keywords: Data Governance, Cybercrime, Digital Sovereignty, Cybersecurity, Digital Transformation.

مقدمة :

تُشكل الثورة التكنولوجية علامة فارقة في عُمر البشرية وذلك انطلاقا من حجم ونوعية الت غييرات التي أضافتها إلى حياة الأفراد والشعوب والدول، وقد أدت هذه الثورة إلى تسريع التحول الرقمي عالميا حيث باتت الدول تعتمد بشكل متزايد على التقنيات الحديثة والتطبيقات الرقمية في شتى مجالات الحياة وقد صاحب هذا التحول توسع غير مسبوق في استخدام الانترنت مما زاد من حجم ومساحة تشابك الدول والمؤسسات مع الشبكة العالمية وأدى إلى ظهور تحديات وتهديدات أمنية جديدة أصبحت تُشكل مصدر خطر متنامي على أمن البيانات الوطنية خاصة تلك الحساسة منها ،وتتعلق هذه التهديدات الأمنية بالجريمة السيبرانية العابرة للحدود ،هذه النوع من الجرائم لا يهدد فقط أمن الأفراد والمؤسسات بل يتمدد تهديده إلى الأمن الوطني والقومي للدول والى إضعاف سيادتها واستباحتها ،وقد دفع هذا الوضع الدول إلى البحث عن استراتيجيات جديدة وفعال ة تُمكنها من السيطرة على بياناتها الوطنية وتأمينها والحد من مخاطر الهجمات الالكترونية دون إغفال الحاجة الماسة للاستفادة من المزايا التكنولوجية والتقنيات الحديثة،من هنا برزت أهمية تَبني إستراتيجية حوكمة إدارة البيانات كنهج فعال قادر على تحقيق توازن دقيق بين استغلال التطور الرقمي وحماية الأمن الوطني وتعزيز السيادة الرقمية،وفي عصرنا الحالي أصبحت البيانات أهم مورد في بناء القو ة وتشكيل النفوذ وبرزت الحاجة الملحة إلى حوكمة فعالة لإدارة البيانات بوصفها أداة استراتيجيه لمواجهة التحديات الأمنية الجديدة وعلى رأسها الجريمة السيبرانية، فمع اتساع رقعة التهديدات الالكترونية وتزايد تعقيدها لم تعد الأساليب التقليدية كافية للتصدي للجريمة الالكترونية بل بات من الضروري الاعتماد على منظومات حوكمة قادرة على تنظيم تدفق البيانات وضمان أمنها وحمايتها من الاستغلال الإجرامي،وبذلك تعتبر حوكمة إدارة البيانات احد الأعمدة الرئيسية في تعزيز السيادة الرقمية للدول حيث تمنحها القدرة على استرجاع السيطرة على فضائها السيبراني وتقليل التبعية للبُنى التحتية الأجنبية بما يعيد التوازن إلى علاقات القوة في المشهد العالمي الجديد الذي بات يُدار عبر الشبكات الرقمية وليست الجغرافية فقط ،وانطلاقا مما سبق نطرح الإشكالية التالية : **كيف تساهم حوكمة إدارة البيانات من خلال مكافحة الجريمة السيبرانية في تعزيز السيادة الرقمية للدول؟**

وللإجابة عن هذه الإشكالية المركزية ينبغي تفكيكها إلى مجموعة من التساؤلات الفرعية التالية :

- ما المقصود بكل من حوكمة إدارة البيانات والجريمة السيبرانية والسيادة الرقمية ؟ وما العناصر الأساسية المكونة لكل منها؟ وكيف تتفاعل هذه المفاهيم فيما بينها؟
- ما طبيعة تأثير الجرائم السيبرانية على السيادة الرقمية للدول؟. وكيف يمكن لحوكمة إدارة البيانات أن تحد من الجرائم السيبرانية وتُسهم في تعزيز السيادة الرقمية للدول؟

وللإجابة على هذه التساؤلات تم اقتراح **الفرضية الرئيسية** التالية:

- ✓ تعتبر حوكمة إدارة البيانات احد أهم الإستراتيجيات الناجعة التي تنتهجها الدول في مواجهه التهديدات السيبرانية وتعزيز السيادة الرقمية.

ولإختبار هذه الفرضية قمنا بوضع الفرضيات الفرعية التالية :

1) إن تحديد العناصر الأساسية لمفاهيم حوكمة إدارة البيانات والجريمة السيبرانية والسيادة الرقمية يؤكد وجود علاقة بنيوية بين هذه المفاهيم ويوضح طريقة التأثير فيما بينها.
2) تتألف السيادة الرقمية من مكونات تتأثر بشكل مباشر بالتهديدات السيبرانية سواء كانت منفردة أو مجتمعة.
3) إن الطبيعة الرقمية للتهديدات السيبرانية لا يمكن التصدي لها بفاعليه إلا من خلال صناعة أنظمة متطورة وبنية تحتية رقمية قويه بالإضافة إلى استراتيجيات أمنية متخصصة.

وتم اعتماد منهج **وصفي تحليلي** لتحديد مفاهيم حوكمة إدارة البيانات و الجريمة السيبرانية والسيادة الرقمية وتفكيك عناصرها وا لعلاقة فيما بينهم و أهميتها، وذلك بالاستناد إلى الدراسات ذات الصلة و إلى أهم الأطر القانونية والتنظيمية المحلية والدولية والى التقارير الرسمية والتجارب الناجحة لبعض الدول ، ومن بين الدراسات السابقة التي ناقشت هذا الموضوع:

1. دراسة بعنوان: نظام كشف التسلل باستخدام تصنيف تدفق البيانات (Intrusion Detection System Using Data Stream Classification) وقد تناولت الدراسة تقديم نظام يقوم على كشف تسلل المجرمين من خلال اعتماده على تصنيف تدفق البيانات وذلك لتحسين الدفاع وصد الهجمات السيبرانية ويدعم تعزيز قدرة الحكومات على مراقبة وتامين البيانات الحساسة ضمن إطار الحوكمة (Abdulmajeed Abdulrahman & Khalel Ibrahem, 2021).

2. دراسة بعنوان: كشف هجمات الرسائل النصية الاحتيالية باستخدام التعلم الآلي (Review Of Smishing Detection Via Machine Learning) وقد تناولت الدراسة استخدام تقنيات التعلم الآليورفع القدرات المعرفية للتقنيات الحديثة للإطار البشري وتوعيته من أجل كشف الهجمات السيبرانية التي تستهدف سرقة البيانات مما يبرز أهمية حوكمة البيانات في حماية المعلومات الشخصية وتعزيز الأمن السيبراني (Rahman Mahmoud & Madjid Hameed, 2023).

لقد تناولت الدراستان نظامان يهدف كل واحد منهما إلى حماية المعلومات وتامين البيانات من خلال كشف الهجمات السيبرانية ومنع سرقه البيانات مما يعزز الأمن السيبراني ويبرز أهمي ة حوكمة البيانات ومن الواضح إن هاتان الدراستان تقنيتان بالأساس ولم تتطرقا إلى تعزيز وحماية السيادة الرقمية ،و هنا يبرز الاختلاف الجوهري مع دراستنا من خلال تركيزنا بشكل أساسي على حوكمة دارة البيانات كأسلوب ناجع وفريد في مكافحه الجريمة السيبرانية وتعزيز السيادة الرقمية.

1. الإطار المفهوماتي للدراسة:

لاشك أن تحديد المفاهيم الأساسية لأي دراسة أكاديمية يُعد خطوة منهجيّ ضرورية وأساسية ،ذلك أن الشرح المفصل لهاته المفاهيم و المصطلحات المستخدمة وفهم أبعادها بشكل دقيق من شأنه أن يُعطي تصور واضح للعلاقة فيما بينها ،لذا يهدف هذا الإطار النظري إلى تقديم شامل لأهم المفاهيم المرتبطة بالدراسة وهي حوكمة إدارة البيانات، الجريمة السبيرانية، والسيادة الرقمية وذلك من اجل تمهيد الطريق لفهم أفضل للإشكالية المطروحة في هذه الدراسة.

1.1. حوكمة إدارة البيانات: قبل الشروع في تحليل دور حوكمة إدارة البيانات في مكافح ة الجريمة السيبرانية وتعزيز السيادة الرقمية من المهم التعرف أولا على طبيعة هذا المفهوم و أبعاده الأساسية لذا سيتم في هذا الجزء التعريف بحوكمة إدارة البيانات واهم أهداف ها والتطرق لأبرز البرامج والسياسات التي تشملها والتحديات المرتبطة بتطبيقها في المؤسسات والدول.

مفهوم حوكمة إدارة البيانات: حوكمة إدارة البيانات واحد من المفاهيم التي راجت في الآونة الأخيرة وكانت موضوع للعديد من الدراسات الأكاديمية وخاصة الأمنية منها وذلك بعد التحول في الأهمية التي اكتسبتها البيانات بحيث أصبحت مورد استراتيجي وركن سيادي وعامل من عوامل الأمن والاستقرار من جهة وعامل من عوامل القوة والنفوذ من جهة ثانية ، لذا ينبغي حمايته والسيطرة عليه ومنع الوصل إليه أو الاستحواذ عليه دون وجه حق،وتُعرف حوكمة إدارة البيانات على أنها مجموعه من الإجراءات الدقيقة والمتكاملة والتي تشمل كل العمليات والبرامج والسياسات والمعايير والأدوار والمسؤوليات التي تضمن إدارة البيانات بطريقه أمن ة وفعالة ومتناسقة ومستدامة داخل المؤسسات وتركز على تمكين المؤسسات من استغلال البيانات من منظور استراتيجي لتحقيق الربح المادي والاستقلالية والسيادة ولدعم اتخاذ القرار السليم وتحقيق كل الأهداف ويمكن إعتبار أن حوكمة إدارة البيانات الرقمية نوع من الإصلاح في سياق التحول الرقمي (Eraly & goransson, 2021) ، الذي يوفر الخدمات بكلفه صفرية.

تعمل إدارة البيانات على التدقيق في البيانات من حيث المضامين والدلالات التي ترمز إليها وعلى اكتمالها بمعنى عدم وجود نقائص عند حجزها أو إدخالها وعلى جعلها متوافر ة فلا يُغلق عليها حيث يمكن الوصول إليها واستغلالها بسهولة من قبل الأشخاص المؤهلين والم رخص لهم وان تكون هذه البيانات فعالة عند استعمالها لذلك أصبحت رهانات حوكمة إدارة البيانات جاذبة للاستثمار الأجنبي للشركات الكبرى والدول العظمى(Diarra & Plane, 2012)،وقد أثبتت بعض الدول مثل سنغافورة فعالي ة كبيرة في تطبيق برامج حوكمة إدارة البيانات، حيث تبنت مبادرة (GovTech) لضمان الجودة العالية والأمان التام للبيانات من خلال توظيف تقنيات الذكاء الاصطناعي وتحليل البيانات اللحظي (Government Technology Agency of Singapore (GovTech))،كما تعد استونيا أحد النماذج الأخرى الناجحة عبر نظامها المعروف بـ (X-Road) الذي يربط جميع البيانات الوطنية بمنصة مركزية محمية بالكامل (Nordic Institute for Interoperability Solutions).

أهداف حوكمة إدارة البيانات وضوابطها وسياساتها: يشهد العالم اليوم تداخلا متزايدا بين الجريمة المنظمة والجريمة ألاقتصاديّ والجريمة السيبرانية إلى جانب تقاطع خطير بين الأنشطة الإجرامية والإرهابية مما يستدعي استجابة شاملة متعددة الأطراف وعابرة للحدود تأخذ بعين الاعتبار متطلبات الأمن الوطني والدولي وكذلك امن الأفراد والمؤسسات وتشير المد لولات السياسية والقانونية إلى جانب الدراسات التكنولوجية والاجتماعية والاقتصادية إلى إن الجريمة السيبرانية لا يمكن مقاربتها وفهمها من منظور أحادي بل إن الفهم المتكامل لهذه الظاهرة يسمح بتبني استراتيجيات وقائية شاملة وفعالة ومتناسقة.

إن الضرورة الملحة اليوم تكمن في تطوير المعرفة الرقمية والمهارات التكنولوجية اللازمة لمواجهه التهديدات السيبرانية المتصاعدة بما يضمن حماية البُنية التحتية الرقمية الحيوية دون المساس بحقوق الإنسان أو تقويض القيم الديمقراطية أو أي من الحريات الأساسية ،غير أن الوعي الجمعي داخل مجتمع المعلومات لا يزال قاصرا عن مستوى التحدي، إذ تظهر المؤشرات أن الأساليب الأمنية التقليدية باتت غير كافيه في ظل ارتفاع وتيرة المخاطر الالكترونية وزيادة تعقيد أدوات الجريمة ،ولذا فان تعزيز قدرات الكشف والتتبع وتحديد الهويات الرقمية إضافة إلى بناء أطر قانونية وتنظيمية وتقنية متقدمة على المستويين المحلي والدولي يعد امرأ حاسما في صد مختلف التهديدات ،كما أن المجرمين يستغلون الثغرات البشرية والتقنية مما يستوجب تطوير جودة البُني المعلوماتية ومتانة نُظم الحماية وفي المقابل قد يُشكل التعاون الدولي و الحوار الهادف و الدبلوماسية السيبرانية أداة ردع غير مباشرة تحد من استخدام الفضاء الرقمي كساحة صراع بين الدول(Ghernaouti, 2023).

وتعتبر أهداف و برامج والسياسات حوكمة البيانات عناصر أساسية لضمان إدارة فعالة وأمنه للبيانات داخل المؤسسات والدول وفيما يلي تفصيل لكل منها :

أهداف حوكمة إدارة البيانات: تهدف حوكمة إدارة البيانات إلى تحقيق مجموعة من الأهداف التي تعزز الكفاءة (Bradshaw, 2025) :

- تحسين جوده البيانات: ضمان أن البيانات المجمعة دقيقه وكاملة وموثوقة مما يقود إلى اتخاذ قرارات صائبة.
- أمن البيانات وحمايتها : حماية البيانات من أي تهديد أو هجمات سيبرانية أو إساءة استخدام.
- الإمتثال للقوانين : تهدف حوكمة إدارة البيانات إلى ضمان تتبع جميع اللوائح القانونية المتعلقة ب سرية البيانات الشخصية وغيرها مما يُغني عن المتابعات القانونية والجزائية .
- تحقيق الشفافية والمساءلة: توضيح المسؤوليات والأدوار المتعلقة بإدارة البيانات لكل موظف مما يزيد من الشفافية والمساءلة داخل المؤسسة.
- تعزيز الابتكار واتخاذ القرارات : استغلال البيانات كمورد استراتيجي للمساعدة في تحسين الأداء المؤسسي ودعم الابتكار.
- زيادة الكفاءة التشغيلية : الاعتماد على نظم رقمية متطورة يتم فيها تنظيم دقيق للبيانات مع البساطة في الإجراءات والعمليات المتعلقة بإدارتها يسمح للمؤسسات من تخفيض في التكاليف وتحقيق اكبر قد من الكفاءة.
- تعزيز الثقة مع العملاء والشركاء: تطبيق حوكمة قوية وناجعة من شأنه أن يُعزز من ثقة العملاء والشركاء التجاريين في المؤسسة وذلك من خلال قدرتها على حماية بياناتهم.

ضوابط حوكمة إدارة البيانات: هي مجموعه المبادرات والخطط التي تنفذ لتحقيق أهداف الحوكمة وضمان استخدام البيانات بكفاءة واقتدار عاليين وتشتمل هذه البرامج على: (الهيئة السعودية للبيانات والذكاء الاصطناعي،2021،ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية،ص 10).

- إدارة الجودة: يعمل على ضمان دقة واكتمال وتناسق البيانات.
- أمن البيانات: يسهر على حماية البيانات من الهجمات السيبرانية والتهديدات الداخلية والخارجية.
- الإمتثال: تلتزم المؤسسات بالامتثال للوائح والقوانين والتشريعات مثل: اللائحة العامة لحماية البيانات (GDPR) وخصوصية المعلومات الصحية (HIPAA).
- إدارة البيانات الوصفية : إن سهولة الوصول إلى البيانات وفهمها تتم عن طريق تنظيم البيانات وتصنيفها وفق منظور محدد وتوصيفها بشكل دقيق بناء على المدلول الذي تحمله.
- تدريب الموظفين: من أهم البرامج التي تقوم عليها حوكمة إدارة البيانات حيث يعمل على توعية الموظفين بالطرق المناسبة لتعامل مع البيانات بشكل آمن وفعال وذلك من خلال العمل على التقليل من الأخطاء البشرية لسد الهفوات والثغرات .
- إستعادة البيانات : وتسمى بالمرونة السبيرانية وذلك من خلال ضمان صمود النظم الرقمية واستمرار العم ل بها واستعادة البيانات بعد وقوع هجمات سيبرانية .

سياسات حوكمة إدارة البيانات: هي الوثائق الرسمية التي توضح القواعد والإجراءات المتعلقة بإدارة البيانات داخل المؤسسات وفيما يلي أهم ها(Porter, 2024):

- امن البيانات : تحدد الطريقة والكيفية التي يتم بها حماية البيانات من الاختراق أو التسريب.
- الوصول إلى البيانات: تحديد قائمة الأشخاص المؤهلين للوصول إلى البيانات بناء على الدور أو الوظيفة.
- إدارة البيانات الشخصية: توضح كيفية التعامل مع البيانات الشخصية بما يتماشى مع القوانين مثل قانون حماية البيانات الشخصية.

- استخدام البيانات: تحدد كيفيه استخدام البيانات ومعالجتها داخل المؤسسة لضمان الشفافية والمسؤولية.
- إدارة دورة حياة البيانات: توضح كيفية جمع واستخدام وإتلاف البيانات بطريقة أمنة ومناسبة.

التحديات التي تواجه حوكمة إدارة البيانات: تُواجه حوكمة إدارة البيانات تحديات أساسية في العديد من المؤسسات في مختلف القطاعات وذلك بسبب الكم الهائل من البيانات التي تأتي من مصادر متعددة ومختلفة وتتمايز في النوعية والجودة وفيما يلي أهم التحديات التي تواجه حوكمة إدارة البيانات (astra, 2025) :

جودة البيانات: التعامل مع البيانات يتطلب التأكد من جودتها وصحتها وغالبا تكون هذه البيانات غير متجانسة أوبها أخطاء أو تناقضات لذلك فتحسين الجودة يشكل تحديا كبيرا لضمان دق ة القرارات المستندة إلى هذه البيانات.

الخصوصية والأمان : إن الكم الهائل للبيانات يجعل من الصعب الحفاظ على خصوصية المعلومات الشخصية وحمايتها من الاختراقات أو سوء الاستخدام لذلك فحوكمة البيانات يجب أن تتضمن الامتثال للتشريعات المتعلقة بالخصوصية مثل:GDPR اللائحة العامة لحماية البيانات.

التكامل والتوافق : تدفق البيانات يأتي من مصادر متعددة مثل قواعد البيانات أو الانترنت أو وسائل التواصل الاجتماعي وغيرها وعملية دمج هذه البيانات وتصنيفها وترتيبها في نظام موحد يشكل احد التحديات الكبر ى لأن هذه البيانات تأتي غالبا بتنسيقات مختلفة وتتطلب معالجة معقدة.

التخزين والمعالجة(التحليل والتفسير) : التعامل مع الحجم الكبير من البيانات يتطلب إمكانيات كبير ة من البُنى التحتية التقنية للقيام بمهام التخزين ثم الانتقال إلى عمليات التحليل والتفسير والذي يتطلب جهودا تقني ة متطورة يتدخل فيها الذكاء الاصطناعي أو الحوسبة السحابية وكذا امتلاك أدوات تحليلية وخبراء متخصصين ذو فعالية وكفاءة عالية لهم القدرة على تفسير كل البيانات واستخراج واستخلاص النتائج والرؤى.

الإمتثال والتشريعات: بعض القطاعات تخضع لقوانين وتشريعات خاصة مثل الصحة التي تتطلب مراعاتها عند استخدام البيانات وعند القيام بعمليات جمع وتخزين البيانات.

المسائلة والملكية: من الضروري وجود آلية شفافة وواضحة تقوم بتحديد المسؤوليات لتمكين عملية المسائلة من خلال تعيين المسؤول عن البيانات لتحديد كيفية استخدامها وهويات من يمكنهم الوصول إليها وكيفية مراقبتها.

التطور السريع في التكنولوجيا: المؤسسات التي تمتلك بيانات كبير ة مطالبة بالتكيف المستمر مع التطور المتسارع للتكنولوجية الرقمية والاستفادة من تحديث الأنظمة لضمان الكفاءة في التعامل مع البيانات.

2.1. الجريمة السيبرانية:

أدى الاعتماد المتزايد على التكنولوجيا الرقمية في مختلف مجالات الحياة إلى ظهور تحديات أمني ة جديدة، تُعد الجريمة السيبرانية من أبرزها وأكثرها تأثيرا على الدول والأفراد على حد سواء ولفهم الأبعاد المختلفة لهذا النوع من الجرائم، وسنعمل على تقديم تعريف واضح للجريمة السيبرانية وتسليط الضوء على ابرز أنواعها بالإضافة إلى استعراض خصائصها الأساسية التي تجعلها تمثل تحديا متزايدا أمام الدول والمؤسسات في العالم الرقمي وتعتبر الجرائم الرقمية المالية من أكثر الجرائم انتشارا بسبب توسع شبكات السلب والنهب المنتشرة على الانترنت والمرتبطة بشبكات الفساد المالي Kleptocracy (Diamond, 2020).

مفهوم الجريمة السيبرانية وأهم أنواعها: ويطلق عليها البعض "الجريمة الالكترونية" وهي استخدام الحواسيب والتكنولوجيا الرقمية للقيام بأعمال غير قانونيه سواء كان ذلك تلاعبا بالبيانات، سرق ة،شن هجمات عبر الانترنت، الابتزاز الالكتروني، أو استخدام التكنولوجية للمساهمة في الجرائم التقليدية ويمثل ذلك أيضا جر يمة مثل : الاحتيال الالكتروني، الاختراقات السيبرانية، وتوزيع البرامج الخبيثة ، و يعود تاريخ مفهوم الجريمة الالكترونية إلى أواخر القرن العشرين مع ازدياد استخدام الحواسيب والانترنت في الجرائم ،يتضمن محاربه هذا النوع من الجريمة استخدام التقنيات المتطورة لتحليل البيانات وتطوير البرامج الأمنية وتكثيف الرقابة على الأنشطة الرقمية وتعزيز التشريعات المتعلقة بجرائم الالكترونية.

وتتسم الجرائم السيبرانية بالتنوع والتعقيد (European Union Agency for Cybersecurity (ENISA), (2020 ، حيث تشمل عدد كبير من الأنشطة غير القانونية والتي يعتمد مرتكبوها على شبكات الانترنت وباستخدام التكنولوجية الرقمية لاستهداف الأفراد والمؤسسات والدول وفيما يلي أهم وأشهر الأنواع واسعة الاستخدام والتي يلخصها الجدول التالي:

الجدول(1): أهم أنواع الجريمة السيبرانية

نوع الجريمة	محتوى الجريمة
الإختراق (Hacking)	هو دخول غير مصرح به وبدون إذن إلى النظم الرقمية والشبكات للوصول إلى بيانات خاصة أو معلومات حساسة و سرية وقد يكون الغرض منها ؛ السرقة،التجسس، التعطيل، التدمير.
الهجمات عبر البرمجيات الخبيثة (Malware Attacks)	تستخدم فيها البرمجيات الضارة كالفيروسات وأحصنة طروادة والديدان وغيرها لإصابة أجهزة الكمبيوتر والشبكات والتطبيقات بهدف التدمير،الغش،الاحتيال، السرقة.
التصيد الإحتيالي (Phishing)	طريقة احتيالية يُستهدف فيها الايميل ويتم بواسطتها خداع المستخدمين بالرسائل المفخخة أوالإعلانات المزيفة للحصول على معلومات حساسة كالكلمات المرور/أرقام البطاقات المالية.
الهجمات الحرمانية (Denial-of-Service-DoS)	يلجأ أصحاب هذا النوع من الهجمات إلى إجهاد النظم الرقمية عند استغلالها بإغراق المواقع أو الخوادم بالطلبات والأوامر لتعطيلها أو إيقافها عن العمل و إخراجها عن الخدمة وحرمان الجمهور والمؤسسات من خدماتها .
التجسس الالكتروني(Cyber Espionage)	الغرض من التجسس الالكتروني هو الحصول على معلومات وبيانات سرية وحساسة ويستهدف فيها الأفراد والمنظمات والدول لتحقيق أهداف وغايات سياسيه أو اقتصادية.
سرقة الهوية (Identity Theft)	تعتبر من أشهر أنواع الجرائم السيبرانية حيث يلجأ مرتكبوها إلى الحصول على المعلومات الشخصية للمستخدمين والاستيلاء عليها عبر الانترنت و توظيفها بطرق غير قانونيه في عمليات فتح حسابات بنكية أو القيام بإجراءات بيع أو شراء باسم الضحية.
الإحتيال الكتروني(Online Fraud):	هي تلك العمليات التي يتم فيها استخدام الانترنيت لتحقيق مكاسب مالية غير مستحقة مثل الاحتيال عبر التسوق الالكتروني أو الاستثمارات المزيفة.
الابتزاز الالكتروني(Cyber Extortion)	السعي إلى الحصول على فدية مالية في مقابل عدم التعرض إلى بيانات الضحايا بالتدمير أو التسريب ويحدث ذلك بواسطة برامج خاصة بالفدية.
استغلال الأطفال عبر الانترنت (Child Exploitation)	يُستغل الأطفال في الفضاء الرقمي للقيام بعمليات الابتزاز سالفة الذكر أو للقيام بنشاط غير قانوني أو إنتاج وتوزيع محتوى غير ملائم.
القرصنة الإعلامية(Piracy)	القيام بعملية توزيع أو استخدام محتوى رقمي محمي بحقوق النشر مثل الأفلام أو الموسيقى أو البرمجيات بدون تصريح بالنشر أو الاستعمال.
الإحتيال البنكي(Banking Fraud)	يتم اللجوء في هذا النوع إلى الهجوم الالكتروني على الحسابات البنكية أو أنظمة الدفع عبر الانترنيت للحصول على الأموال بطريقة غير مشروعة.
الإرهاب السيبراني(Cyber Terrorism)	وهو أخطر أنواع الجرائم السيبرانية كونه يقوم بتوظيف التكنولوجية الرقمية للقيام باستهداف الأمن القومي للدول بطريقة مباشرة أو غير مباشرة ويتم ذلك عن طريق التهديد أو بتنفيذ هجمات تهدف إلى الإضرار بالبُنى التحتية الحيوية.

المصدر: تم إعداد الجدول بناءا على المعلومات الواردة في (جربوعة وبوطمين، 2023)

خصائص الجريمة السيبرانية: تُعرف الجريمة السيبرانية (Cybercrime) بأنها الأنشطة غير القانونية التي تُرتكب باستخدام الانترنت أو الأنظمة الرقمية تتميز هذه الجرائم بعدد من الخصائص الفريدة التي يلزم لمواجهتها استراتيجيات مبتكرة ومتقدمة بما في ذلك التوعية ،التحديث المستمر للأنظمة الأمنية والتعاون الدولي الفعال وفيما يلي نذكر أهمها(مراد و شويرب، 2023) :

الاعتماد على التكنولوجية: تعتمد بشكل رئيسي على الوسائل التكنولوجية مثل الحواسيب والشبكات والهواتف الذكية والانترنت، كما يمكن أن تُرتكب من أي مكان في العالم بفضل طبيعة البني الرقمية المترابطة.

صعوبة التتبع: غالبا ما يقوم مرتكب الجرائم بإخفاء هويتهم باستخدام تقنية مثل الـ VPNأو برامج التشفير ، وقد ترتكب من أماكن بعيده جغرافيا عن موقع الضحية مما يعقد عمليه التتبع والقبض عليهم (جربوعة و بوطمين، 2023).

الأضرار غير المادية: في كثير من الجرائم السيبرانية لا تكون الخسائر في شكل أضرار مادية بل تظهر في صورة فقدان بيانات أو إنتهاك للخصوصية أو تسريب لمعلومات حساسة أو خسارة السمعة التجارية للمؤسسات كما أنه يمكن أن تؤدي إلى خسائر مادية ضخمة نتيجة الاحتيال أو القرصنة المصرفية أو غيرها.

سهوله تنفيذ: توفر بعض الأدوات على الانترنت المُظلِم (Dark Web) تسهيلات للمجرمين مثل البرمجيات الضارة الجاهزة الاستخدام، كما أن بعض الهجمات يتم تنفيذها ببرمجيات ووسائل بسيطة و محدودة مما يجعلها متوفرة ومتاحة للأفراد وللمجموعات الصغيرة.

التأثير العالمي: يمكن أن تتم مهاجمة أفراد أو مؤسسات أو دول في مناطق مختلفة و في نفس الوقت، والجرائم السيبرانية معقدة وعابرة للحدود والوصول إلى مرتكبيها يستدعي التعاون الدولي في التحقيقات .

سرعه التنفيذ والانتشار: تنتشر الجرائم السيبرانية بسرعة كبيرة جدا مثل انتشار البرمجيات الخبيثة أو الشائعات الكاذبة، وتلحق الجرائم السيبرانية أضرارا ضخمة خلال وقت قصير مقارنة بالجرائم التقليدية.

صُعوبة الإثبات القانوني: تحتاج التحقيقات إلى خبراء في الجرائم الرقمية لتوثيق الأدلة وغالبا ما يتم استخدام أدلة رقمية يصعب جمعها والتحقق من صحتها ، كما يجب على المحققين التعامل مع التحديات المتعلقة بالتشريعات والقوانين المختلفة في الدول التي قد يكون المجرم أو الضحية فيها.

التطور المستمر: يعتمد المجرمون باستمرار على التطور التكنولوجي والرقمي لتطوير الأساليب التي يستخدمونها أثناء تنفيذهم لهجماتهم مما يجعل من الصعب على الأجهزة الأمنية مواكبتها بسرعة.

3.1. السيادة الرقمية:

تُعتبر السيادة التقليدية أحد الأركان الأساسية لـ لدولة باعتبارها الكيان الذي يتمتع بكامل سلطاته دون خضوع لإكراه خارجي ،وهي بهذا المفهوم تمتلك كامل حرية التصرف والاستقلال في اتخاذ القرار،وفي الفضاء الرقمي يمكن تعريف السيادة الرقمية بأنها القدرة على تطوير التكنولوجية الرقمية والتحكم فيها بحرية واستقلالية، غير أن السيادة لا تقاس فقط بالقدرة القانونية بل تتجاوز إلى المحافظة على توازن القوى وفي البيئة الرقمية تتجلى هذه السيادة أحيانا في شكل تفوق معرفي تكنولوجي بين من يمتلك أدوات الرقمنة ومن يُقصى إلى هوامشها فمنذ التسعينيات ومع تصاعد النشاط الرقمي أعيد تشكيل موازين القوى بشكل غير مسبوق وبرز فاعلون جدد كالشركات التكنولوجية الخاصة التي باتت الدول نفسها تعتمد عليها حيث تراجعت الحدود الوطنية التقليدية في إدارة الفضاء السيبراني مما قيد السيادة الكلاسيكية في هذا الإطار تمثل التكنولوجيا الرقمية أداة مزدوجة تجمع بين القوه الناعمة بما فيها التأثير الثقافي والمعرفي والقوة الصلبة المرتبطة بالإكراهات الاقتصادية والعسكرية واليوم تتصدر الولايات المتحدة والصين مشهد السيادة الرقمية بفضل تفوق شركاتهما الكبرى ومراكز أبحاثهما المتقدمة (Bellanger & Thida Norodom, 2023).

مفهوم السيادة الرقمية: تُشكل السيادة الرقمية احد أهم المفاهيم الحديثة التي برزت نتيجة التوسع السريع باستخدام التكنولوجيا الرقمية واعتماد الدول المتزايدة على الفضاء الالكتروني وفي ظل تنامي التحديات المرتبطة بالبيانات الوطنية أصبح من الضروري التعرف بشكل دقيق على مفهوم السيادة الرقمية وتحديد مكوناتها الرئيسية وإبراز أهميتها في حماية استقلاليه الدول ومصالحها الوطنية من التهديدات الرقمية المتنوعة.

و تُعرف السيادة الرقمية بأنها قدرة الدولة على ادارة بياناتها والتحكم في بنيتها التحتية الرقمية بهدف تحقيق الاستقلال الرقمي وتأمين مصالحها الوطنية وحمايتها من المخاطر والتهديدات التي تواجهها في الفضاء الالكتروني(شرقي، 2023)، وتعكس قدر ة الدولة على التحكم في بياناتها الوطنية وتنظيم بنيتها الرقمية من خلال وضع السياسات والتشريعات التي تضمن أمن المعلومات وحمايتها وتسعى كذلك إلى تنظيم تدفق البيانات واستخدامها بشكل مستقل بما يقلل من الاعتماد على الجهات التكنولوجية الخارجية ويعزز من استقلاليه الدولة في ادارة مواردها الرقمية(شرقي، 2023).

مكونات السيادة الرقمية: تشير السيادة الرقمية إلى القدرة على السيطرة والتحكم في الموارد الرقمية والمعلومات التي تُنتج أو تَمر عبر نطاقهم ،هذا المفهوم يرتبط بالحفاظ على استقلالي ة الدولة في العالم الرقمي وضمان أمن وخصوصية بياناتها وتشمل السيادة الرقمية على عدة مكونات رئيسية هي: (الشرشابي ،مركز الأمن السيبراني للأبحاث والدراسات ،2025)

السيادة على البيانات: التحكم في مكان تخزين البيانات والسيطرة عليه(على خوادم محلية أو خارجية)، ووجود الإطار القانوني والتشريعي الذي يضبط الكيفية التي يتم بها جمع ومعالجة البيانات الشخصية، وكذلك الإشراف والتحكم في مشاركة البيانات المحلية مع أطراف خارجية (مثل الشركات الأجنبية). (الشرشابي ،مركز الأمن السيبراني للأبحاث والدراسات ،2025)

السيادة على البنية التحتية الرقمية: تكمن استقلالية الدولة في امتلاك شبكات الاتصالات وخدمات الانترنيت والقدرة على تطويرها، وحيازة تكنولوجية رقمية محلية قادرة على تخزين البيانات وتقديم الخدمات مثل الخوادم والمنصات داخليه، إضافة إلى تقليل الاعتماد على الشركات الخارجية لإدارة البنية التحتية الأساسية. (الشرشابي ،مركز الأمن السيبراني للأبحاث والدراسات ،2025)

الأمن السيبراني: ويعني تطوير أنظمة قوية لحماية الشبكات الوطنية من الهجمات السيبرانية ، و إنشاء استراتيجيات لمواجهة التهديدات الرقمية مثل التجسس والقرصنة، وكذلك تامين العمليات الحكومية الرقمية.

التشريعات والقوانين الرقمية: وهو وضع قوانين وطنية تنظم الفضاء الرقمي مثل قوانين حماية البيانات الشخصية، وضمان أن تكون هذه القوانين متوافقة مع المعايير الدولية مع مراعاة السيادة الوطنية، إضافة إلى التفاوض على اتفاقيات دوليه بما يتوافق مع مصلحة الدولة.

التحكم في التكنولوجيا والمنصات: امتلاك منصات وطنية للتواصل الاجتماعي و محركات للبحث و البريد الالكتروني، و تطوير البرمجيات والتطبيقات المحلية لتقليل الاعتماد على المنتجات الأجنبية ، اضافة إلى دعم البحث والتطوير لتعزيز الابتكار التكنولوجي المحلي.

التعليم والوعي الرقمي: الوعي حول أهمية حماية البيانات الشخصية والسيادة الرقمية، و إدراج مناهج تعليمية تهدف إلى تعزيز الثقافة الرقمية، ودعم برامج التدريب في مجال الأمن السيبراني والذكاء الاصطناعي.

الشركات الدولية والتأثير الجيوسياسي: المساهمة في صياغة وتشكيل المعايير الدولية المتعلقة بتسيير الفضاء الرقمي كقوانين الانترنت ، والانخراط في مبادرات التعاون والتنسيق الدولي لضما ن امن واستقرار الفضاء الرقمي، والتويع في المصادر التكنولوجية وعدم الاعتماد بشكل كامل على تقنيات من دول بعينها لتحقيق توازن جيوسياسي. (الشرشابي ،مركز الأمن السيبراني للأبحاث والدراسات ،2025)

أهمية السيادة الرقمية:

تتجلى أهمية السيادة الرقمية في امتلاك الدول القدرة على التحكم الكلي في بنيتها التحتية وبيانات مواطنيها، الشيء الذي يمكن من حماية الخصوصية الأفراد وامن البيانات ويدعم الاستقلال الرقمي والتكنولوجي والاقتصادي في مواجهة التهديدات السيبرانية والتدخلات الأجنبية ،كما تساهم السيادة الرقمية في قدرة الدولة على التأطير القانوني والتنظيمي للفضاء الرقمي بما يحفظ مصالحها الوطنية وينسجم مع تطلعات مواطنيها للانخراط في الحياة الرقمية ومن بين الجوانب المهمة التي تشكل أهمية السيادة الرقمية ؛ الأمن الوطني: حماية الأنظمة الرقمية والبُنى التحتية الحساسة من التهديدات الخارجية، حماية الخصوصية: ضمان حقوق الأفراد في حماية بياناتهم و التحكم فيه، تعزيز الاقتصاد المحلي: دعم الشركات التكنولوجية المحلية والتقنيات الوطنية ، الاستقلالية التقنية: تقليل التبعية للخدمات والتقنيات الأجنبية غير أنها قد تواجه عدة تحديات كبرى أهمها:

التبعية التكنولوجية للشركات الكبرى: يمثل النفوذ المتزايد للشركات متعددة الجنسيات خاصة عمالقة التكنولوجيا شكلا جديدا من أشكال الإستعمار غير التقليدي ،حيث لا تمارس السيطرة من خلال الجيوش أو الاحتلال بل عبر الهيمنة على البيانات والخوارزميات والبُن ى التحتية الرقمية التي تعتمد عليها المجتمعات الحديثة ،هذا " الاستعمار السيبراني " كما يسميه الفيلسوف إيريك سادين يعيد تشكيل علاقات القوة في العالم،إذ تصبح الشركات التكنولوجية فاعلا سياسيا واقتصاديا له سلطه تتجاوز أحيانا سلطه الدول وتفرض منطقه ا التقني على الحياة اليومية والقرار العام، إن اعتراف الدنمارك في سنه 2017 بضرورة تعيين "سفير"لدى شركات وادي السيليكون ،حيث لم تعد السيادة حِكرًا على الدول بل باتت متنازعة بين الحكومات وكيانات رقمي ة تمتلك مفاتيح العالم المعاصر (Türk, 2020).وتعتمد الدول المتأخرة رقميا على الخدمات التكنولوجية من الشركات العالمية مثل : Google, Microsoft, Amazon في مجالات الحوسبة السحابية والذكاء الاصطناعي وإدارة البيانات الحكومية مما يجعل هذه الدول عرض ة لمخاطر فقدان السيطرة على بياناتها الوطنية على سبيل المثال في سنة 2020 واجهت الحكومة الفرنسية جدلاً حول الاعتماد المفرط على الخدمات السحابية من شرك ة ميكروسوفت مما أدى إلى طرح مشروع سحابة وطنية للحد من هذه التبعية(Desmarais, 2025)، ويشير مصطلح GAFAMs إلى عمالقة التكنولوجيا الخمسة الكبار في العالم الرقمي وهم : Google, Apple, Facebook,(Meta),Amazon, Microsoft وتمثل هذه الشركات مراكز قو ة اقتصادية وتكنولوجية هائلة تتحكم في البنية التحتية للانترنت والخدمات السحابية و محركات البحث ومنصات التواصل الاجتماعي والتجارة الالكترونية والبرمجيات وقد أصبحت لاعبا جيو سياسيا مؤثرا يتجاوز دور الدول أحيانا خاصة فيما يتعلق بالسيادة الرقمية وحوكمة البيانات والتأثير في الرأي العام وبفعل قدرتها المالية والتقنية باتت هذه الشركات محورا للنقاش العالمي حول الاحتكار وحماية الخصوصية والتنظيم القانوني للفضاء السيبراني.

التهديدات السيبرانية المتزايدة: لا شك أن استمرار الدول في الانخراط في الشبكات العالمية يُضاعِف من الهجمات الالكترونية التي تستهدف البُنى التحتية لهذه الدول وخاصة الحساسة منها مثل قطاعات الأمن والمالية والطاقة والاتصالات وغيرها(جعيجع، 2017، ص 73).

نُقص التشريعات المحلية الملائمة: التخلف التكنولوجي والرقمي لبعض الدول يصاحبه غياب في النصوص التشريعية والقانونية الشاملة لتنظيم الفضاء الرقمي وحماية البيانات.

التنافس الدولي : في إطار اشتداد التنافس الدولي تلجا الدول الكبرى إلى سن قوانين وسياسات تفرض من خلالها على شركاتها التعاون مع أجهزة استخباراتها لتمكينها من الوصول إلى جميع البيانات التي لديها (هادي، 2023، ص 117)،ويتم ذلك وفق برامج ومشاريع تُمكن الأجهزة المختصة من الولوج إلى قواعد البيانات التي تحوزها هاته الشركات الكبرى والحصول على كل البيانات المطلوبة (جعيجع،2017، ص141) ، وهو ما يعتبر انتهاكا صريحا لسيادة الدول الأخرى على بياناتها.

التطور المتسارع في التكنولوجيا: يُشكل التطور السريع في أدوات الفضاء الرقمي وفي وسائل الذكاء الاصطناعي اكبر تحدي للعديد من الدول التي تقف عاجزة عن مواكب ة التطور الشيء الذي يخلق فجو ة رقمية(هادي، 2023، ص 117).

نقص الكفاءات المحلية في المجال الرقمي: يُعتبر نقص الكفاءات المحلية احد التحديات الكبرى التي تواجه تحقيق السيادة الرقمية،ولذلك ينبغي على الدول ال تي تسعى لـلقضاء على الفجوة الرقمية والسيطرة على بياناتها الحساسة،العمل وفق برامج خاصة على تكوين إطارات وكفاءات وطنية متخصصة ومن خلالها خلق كيانات رقمية للاستغناء تدريجيًا على الكفاءات والكيانات الأجنبية.

الحروب السيبرانية والجيوسياسية: الفضاء الرقمي أصبح ميدانا للمنافسة وساحة للصراع بين الدول وذلك في إطار التحول في مفهوم القوة والنفوذ ،مما يُعقد من مسالة السيادة الرقمية ويضاعف من حجم التحديات.

2. تأثير الجريمة السيبرانية على السيادة الرقمية:

تُؤثر الجريمة السيبرانية بشكل مباشر على قدرة الدول في الحفاظ على سيادتها الرقمية،فقد أظهرت تجارب العديد من الدول كيف تؤدي الهجمات السيبرانية إلى فقدان السيطرة على بياناتها الوطنية مثل حادث ة التدخل الروسي في الانتخابات الأمريكية سنة 2016 (عودة، 2018)، والتي تسببت في أزمة سياسية كبرى ،وكذا الهجمات التي استهدفت البنية التحتية في أوكرانيا سنة 2021 ،مما اثر على استقلالها الرقمي بشكل خطير(البهي، 2022).تمثل الجريمة السيبرانية تحديا كبيرا للسيادة الرقمية للدول إذ تؤثر في مختلف الجوانب السياسية،الاجتماعية،الاقتصادية،الأمنية والعسكرية، يعتمد استقرار الدول على تامين فضائها الرقمي من التهديدات وتجنب الاختراقات التي تعرض بياناتها الحيوية و بيانات مواطنيها للخطر.

1.2. الآثار السياسية والاجتماعية:

تمثل الجريمة السيبرانية أحد أكبر التحديات التي تواجه الدول في الفضاء الرقمي،إذ تتعدى تأثيراتها مجرد الخسائر التقنية والمادية فقط لتشمل أبعادًا سياسية واجتماعية عميقة، سنقدم هنا تحليل الأثر السياسي للجريمة السيبرانية من خلال استعراض كيفيه استغلالها في إحداث إضطرابات سياسية إضافة إلى بيان تأثيراتها الاجتماعية السلبية على استقرار المجتمعات والثقة العامة.

- **زعزعة الثقة في الحكومة والمؤسسات العامة :** الهجمات السيبرانية التي تستهدف المؤسسات الحكومية من أجل إيقاف النظام الرقمي أو لتعطيل الخدمات أو غيرها من الأهداف التخريبية تؤدي إلى فقدان ثقة المواطنين في الدولة من خلال عدم قدرتها على حماية بياناتهم ومصالحهم ،مثل ما حدث في سنغافورة سنة 2018 عندما تم استهداف السجلات الصحية وأدى ذلك أدى إلى اهتزاز الثقة في قدرة الحكومة على حماية البيانات الشخصية للمواطنين(Kim & Aravindan, 2018).
- **التلاعب في الانتخابات والتدخل الأجنبي:** لم تسلم العملية الانتخابية من الهجمات السبيرانية حيث يتم إستغلال الفضاء الرقمي من أجل التأثير في الانتخابات عبر توجيه الرأي العام أو التلاعب بالمعلومات أو سرقة البيانات والتعديل عليها لتحقيق نتائج معينة ، وهو الذي حدث في الانتخابات الرئاسية الأمريكية في نوفمبر 2016 عندما تم التدخل الروسي بعد نشر معلومات مضللة واختراق البريد الالكتروني لمسؤولين سياسيين كبار(عودة، 2018)،وفقا لتقرير: ENISAسنة 2020 ، وقد كانت عمليات التظليل ونشر الأخبار الكاذبة عبر الفضاء الرقمي إحدى ابرز التحديات التي واجهت الانتخابات الأوروبية الأخيرة مما نشير إلى تزايد الأثر السياسي للجريمة السيبرانية(European Union Agency for Cybersecurity (ENISA), 2020).
- **التجسس السياسي والدبلوماسي:** يُعد التجسس الإلكتروني أحد ابرز التهديدات السياسية التي تؤثر في سيادة الدول حيث يعتبر سلاح فتاك طالما يتم استهداف النظم الرقمية الخاصة والعامة للحصول على معلومات سرية غير قابلة للتداول العام ،وفي شهر نوفمبر من سنة 2010 هزت التسريبات المعلوماتية أركان عديد الحكومات والدول والذي عُرف بوثائق ويكيليكس، والتي قامت بنشر الآلاف من الوثائق الدبلوماسية السرية وخلفت امتعاضا كبيرا من قبل الدول والحكومات (جعيجع، 2017، صفحة 131)، وكذا وثائق بنما في سنة 2016 ، إلا أنه تجدر الإشارة برامج التجسس البرامج الأمريكية الشهيرة: إيشلون و بريزم، ومجموعة الفيروسات الروسية : تورلا (جعيجع، 2017، ص 131) ، كما يُعد برنامج التجسس الإسرائيلي "بيغاسوس" من أشهر برامج التجسس التي تم الكشف عن استخدامها سنة 2021 على نطاق واسع من قبل عدة حكومات لمراقبة سياسيين ودبلوماسيين وصحفيين مما أدىإلى توترات دبلوماسيه واسعة(Tidy, BBC News, 2021).

الآثار الاجتماعية:

- **نشر الأخبار الكاذبة والمعلومات المظ لة :** من بين خصائص الفضاء الرقمي سرعة انتشار المعلومة أو تداول الخبر ،وعندما يتم استهداف المجتمع بأخبار مغلوطة أو إشاعات كاذبة ستؤدي حتما هاته المعلومات

المظُللة إلى اضطرابات اجتماعيه وأ عمال عنف خاصة إذا كانت البنية الاجتماعية هشة أو هناك توترات طائفية أو عرقية ، وقد أدت رسائل كاذبة ومضللة على الواتساب في الهند سنة 2018 إلى أعمال عنف طائفي وقتل وتخريب في عدة مناطق(Satish, 2018).

- **انتهاك الخصوصية:** تستهدف الجرائم السيبرانية في معظم الحالات البيانات وخاصة البيانات الشخصية ، والتي تؤدي إلى تسريب المعلومات الشخصية،الأمر الذي يُعتبر انتهاكا واضحا للخصوصية ويدفع إلى فقدان ثقة الأفراد في الخدمات الرقمية، وذلك لعجز النظم الرقمية عن حماية بياناتهم الشخصية، وقد أدى هجوم سيبراني سنة 2021 إلى تسريب بيانات 533 مليون مستخدم من منصة الفيسبوك وانتشرت بياناتهم الحساسة على نطاق واسع وأثارت الحادثة قلقا اجتماعيا كبيرا(Dellinger, 2021).
- **التهديدات المجتمعية:** إن استهداف الجرائم الالكترونية للخدمات الحيوية مثل الصحة والاتصالات وغيرها بأي شكل من أشكال الإستهداف يُؤدي إلى اضطرابات اجتماعيه ،مثل استهداف خدمات الطوارئ الصحية في السويد سنة 2022 ،مما أدى إلى توقف خدمات الإسعاف وأثار قلق اجتماعي واسع.

2.2. الآثار الاقتصادية والتكنولوجية : أصبح الاقتصاد والتكنولوجيا في مقدمة القطاعات المتضررة من الجرائم السيبرانية،حيث تؤدي هذه الجرائم إلى خسائر مادي ة كبير ة والى تقويض الثقة في الاقتصاد الر قمي الوطني،وهنا سنتطرق إلى توضيح أثار الجريمة السبيرانية الاقتصادية والتكنولوجية عبر التركيز على الخسائر المالية انخفاض الثقة الاقتصادية والتحديات التي تواجه التطور التكنولوجي.

الآثار الاقتصادية:

- **خسائر مالية مباشرة :** تؤدي الهجمات السيبرانية على الشركات والمؤسسات الاقتصادية إلى سرقة الأموال أو تعطيل الأنظمة ،مما يُسبب خسائر مالية مباشرة،مثلما حدث سنة 2022 عندما تعرضت منصة تداول العملات الرقمية FTX إلى الاختراق، تكبدت على إثرها خسائر مالية تجاوزت 400 مليون دولار وانهيار كامل للمنصة(Hoskins, 2023)،وبحسب تقرير IBM سنة 2021 ، إرتفعت تكلفة اختراق البيانات الواحدة إلى مستويات قياسيه حيث بلغ متوسطها 4. 24 مليون دولار مما يؤكد الأثر الاقتصادي الخطير للجريمة السيبرانية(IBM , 2021).
- **انخفاض الثقة في الاقتصاد الرقمي:** تؤدي الهجمات السيبرانية إلى تراجع الاستثمارات في الاقتصاد الرقمي، مما يؤثر ذلك على النمو الاقتصادي ،كما حدث بعد انهيار بنك سيليكون فالي (SVB) سنة 2023 والذي رافقه محاولات احتيال إلكترونية أدت إلى انخفاض حاد في الثقة بالقطاع المصرفي الرقم ي(الجزيرة الاخبارية، 2023).
- **ارتفاع التكاليف التشغيلية :** السعي إلى تعزيز الأمن السيبراني يتطلب استثمارات ضخمة في التكنولوجيا وفي البُنى التحتية الرقمية وتشجيع الابتكار ،وهذا يتطلب تخصيص حزم مالية كبيرة تؤثر على الاقتصاد الوطني.

الآثار التكنولوجية:

- **تعطيل الابتكار:** الهجمات التي تستهدف أبحاث الشركات والمؤسسات البحثية يمكن أن تعرقل الابتكار وتمنع التطور التكنولوجي ،ففي شهر جويلية من سنة 2020 تعرضت شركه Garmin لهجوم الكتروني بالفدية أدى إلى تعطيل خدماتها الرقمية بشكل كامل ، مما أوقف عمليات تطوير منتجات جديدة لفترة طويلة (Tidy, BBC News, 2020).
- **سرقة الملكية الفكرية:** القرصنة هي وجه من أوجه الجرائم السبيرانية وهي عبارة عن هجوم يتم من خلاله الحصول على بيانات من غير وجه حق وتكون في الغالب معلومات حساسة ومنجزات خاصة بأصحابها وجهود فكرية وعلمية ، مثل سرقة التكنولوجيا والأسرار التجارية مما يؤثر سلبا على القدرة التنافسية الوطنية.
- **تقويض الاستقلال التكنولوجي:** رغم إجراءات الحماية المتبناة فإن الاختراق المتكرر يؤدي إلى الشعور بعدم الأمان الرقمي وهو ما يدفع الدول إلى الاعتماد على التكنولوجيا الأجنبية،مما يضعف سيادتها الرقمية.

3.2. الآثار الأمنية والعسكرية:

تتجاوز الآثار الناجمة عن الجرائم السيبرانية حدود المجال الرقمي لتشكل تهديدا مباشرا للأمن القومي حيث باتت الهجمات الالكترونية عنصرا رئيسيا في النزاعات الدولية المعاصرة وتمتد هذه التهديدات إلى القطاعات العسكرية م ستهدفة بذلك البُنى التحتية الدفاعية للدول ،لذا سيركز هذا الجزء على الآثار الأمنية

والعسكرية لهذه الجرائم من خلال استعراض ابرز المخاطر والتحديات التي تواجه امن الدول وقواتها العسكرية في الفضاء الرقمي.

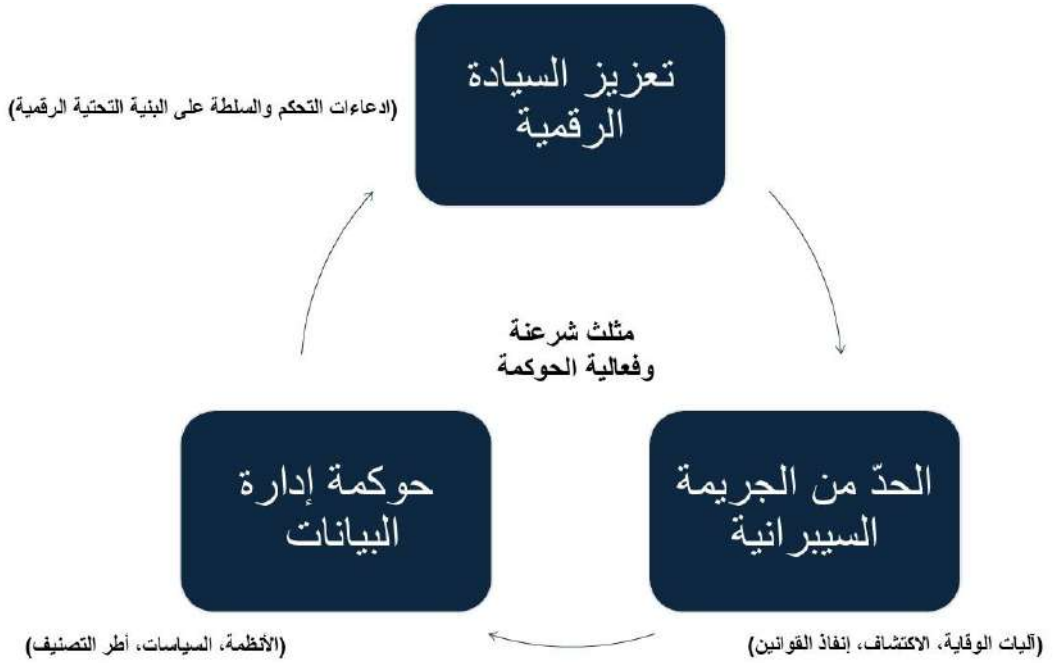
الآثار الأمنية:

- **تهديد الأمن القومي :** الهجمات السيبرانية التي تستهدف الأنظمة الحيوية كالمطارات والمستشفيات و شبكات الطاقة تهدد الأمن الداخلي ،ففي شهر ماي من سنة 2021 تعرض قطاع الصحة في ايرلندا إلى هجوم فديةٍ الكتروني (Ransomware)،أدى إلى إيقاف شبكات المستشفيات والخدمات الطبية لمد ة أسبوع كامل مما سبب اضطرابا صحيا خطيرا في البلاد (Corera, 2021).
- **الابتزاز الالكتروني:** تلجأ م جموعات القر اصنة إلى مهاجمة المواقع الحساسة للدول وذلك للقيام بابتزاز الحكومات والشركات مما يضعف قدرتها على اتخاذ قرارات مستقلة،ففي شهر ماي من سنة 2021 هاجمت مجموعه من القراصنة شركة "Colonial Pipeline" في الولايات المتحدة الأمريكية مما أدى إلى توقف إمدادات الوقود الرئيسية في البلاد واجبر الشركة على دفع فدي ة قدرها 4,4 مليون دولار (Watson & Images, 2021).
- **اختراق قواعد البيانات الحكومية :** تُعد قواعد البيانات الحكومية أهدافا رئيسية للهجمات السيبرانية ،حيث يؤدي اختراقها إلى تسريب معلومات حساسة تؤثر على امن الدولة ،مثلما حدث سنة 2023 حين تعرضت الحكومة الأمريكية لإختراق سيبيراني استهدف البريد الالكتروني الخاص بوزارة الخارجية وتم تسريب مراسلات دبلوماسيه حساسة أثرت على الأمن الدبلوماسي (Lyngaas, 2023).

الآثار العسكرية:

- **تعطيل الأنظمة العسكرية :** يمكن للهجمات السيبرانية استهداف وتعطيل الأنظمة والبُنى التحتية العسكرية ما يشكل تهديدا حقيقيا للجاهز يةٍ الدفاعية للدول ،ففي شهر فبراير من سنة 2022 شنت روسيا هجمات الكترونية واسعة استهدفت أنظمة الاتصالات العسكرية الأوكرانية قبل وأثناء بداية الغزو الروسي لأوكرانيا مما أدى إلى عرقله قدر ة الجيش الأوكراني على التواصل وإدارة العمليات بشكل فعال (The Guardian, 2022).
- **التجسس العسكري:** تُمثل الهجمات السيبرانية وسيلة فعالة للحصول على معلومات عسكريةٍ حساسة تُضعف من قدرة الدولة على التخطيط العسكري والسياسات الدفاعيةٍ ففي سنة 2021 كشفت السلطات الأمريكية قيام قراصنة تابعين لدولة أجنبية باختراق شبك ة معلومات سريةٍ تخص أنظمة دفاعية أمريكية مما أدى إلى حصولهم على معلومات حساسة حول القدرات الدفاعية والاستراتيجيات العسكرية الأمريكية (Cimpanu, 2022)، كما أشار تقرير IBM X-Force لسنة 2021 إلى تصاعد هجمات التجسس الالكتروني التي تستهدف القطاعات الحكومية والعسكرية مما يبرز الخطر الأمني المتزايد لهذه الهجمات على سيادة الدول الرقمية(IBM , 2021).
- **الحرب السيبرانية :** أصبحت الهجمات الإلكترونية جزء لا يتجزأ من استراتيجيات الحروب الحديثة،إذ تُستخدم لتعطيل القدرات العسكرية للخصوم دون الحاجة للاشتباك العسكري التقليدي ،فعندما قامت إيران بهجوم إلكتروني على ألبانيا في شهر جويلية من سنة 2022 أدى ذلك إلى تعطيل الخدمات الحكومية بشكل كامل وإغلاق السفرات والمواقع الالكترونية الرسمية،مما دفع بحلف الناتو للتدخل والمساعدة في الدفاع عن الأمن السيبراني الألباني (Reuters, 2022).

الشكل (1): نموذج العلاقة الثلاثية بين إدارة حوكمة البيانات للحد من الجريمة السيبرانية وتعزيز السيادة الرقمية



المصدر : الباحِثَين

3.فعاليه حوكمة إدارة البيانات في التصدي للجريمة السيبرانية والتامين السيادة الرقمية :

إ ن نجاح تطبيق حوكمة إدارة البيانات ليس مرهونا فقط بتوفر تكنولوجيا بل يرتبط أيضا بعوامل سياسية واقتصادية واجتماعية ينبغي مراعاتها عند رسم استراتيجيات وطنيه للأمن السيبراني (علي فهمي و يوسف هاشم، 2024)، إلا أن حوكمة إدارة البيانات تُمثل ركيزة أساسية لمواجهة الجرائم السيبرانية وتعزيز السيادة الرقمية للدول، حيث تعمل على تنظيم عمليات جمع البيانات وتخزينها واستخدامها بطريق ة آمنة،وهو ما يساهم بشكل مباشر في الوقاية من الهجمات السيبرانية والتصدي الفعال لها والسيطرة على البيانات الوطنية بما يضمن استقلالية القرار وحماية الموارد الرقمية للدولة.

1.3 الوقاية من الجرائم السيبرانية : تُعد الوقاية الخطوة الأولى والاهم في إستراتيجية حوكمة إدارة البيانات وتهدف إلى الحد من فُرص حدوث الجرائم السيبرانية من خلال اتخاذ التدابير و الإجراءات الاستباقية وتتحقق بـ:

- **تطبيق معايير الأمن السيبراني :**اعتماد المعايير الدولية المتخصصة في إدارة امن المعلومات(مال الله عبد الله و حسن الناصر) ، مثل معيار : ISO/IEC 27K،تعزيز ثقافة الأمن السيبراني داخل المؤسسات من خلال سياسات واضحة وصارمة لحوكمة إدارة البيانات.
- **التدريب ونشر الوعي:** تدريب الموظفين على أساسيات الأمن السيبراني و كشف محاولات التصيد الالكتروني وتعريفهم بأهم أساليب الحماية منها، وإطلاق حملات توعوية عام ة حول أهمية حماية البيانات الشخصية ومخاطر التساهل في التعامل معها.
- **تشفير البيانات وحمايتها:** استخدام تقنيات تشفير قويه لحماية البيانات إثناء تخزينها أو نقلها ، و تطبيق سياسات تحدد صلاحيات الوصول للبيانات بناء على ادوار المستخدمين ومسؤولياتهم.
- **ادارة المخاطر والتقييم المستمر :** " هي عملية قياس وتقييم للمخاطر وتطوير استراتيجيات لإدارتها ... تعني فهم العمليات الجارية ،والاستجابة للعوامل التي تحدث ضرر بها ،أو تؤثر سلبا عليها ،أو على المعلومات الناتجة منها ... كما يمكن تعريفها بأنها النشاط الإداري الذي يهدف إلى التحكم بالمخاطر وتخفيضها إلى مستويات مقبولة ... هي عملية تحديد وقياس وتخفيض المخاطر التي تواجه الشركة أو المؤسسة، والسيطرة عليها " (بن حسن العريشي و حسن الشلهوب، 2016، ص 54-55)، وتتضمن إدارة المخاطر عمليتين أساسيتين؛ **الأولى تحليل المخاطر:** لتحديد التهديدات بدقة وما ينتج عنها من مخاطر ، من أجل وضع الآليات المناسبة للتحكم في المخاطر أو للتقليل من أثارها أو تحييدها نهائيا (بن حسن العريشي و حسن الشلهوب، 2016، ص 57)،وتقوم بدورها على ثمانية خطوات متتالية ويمكن أن يتم بعضها بالتوازي

وهي؛ تقييم النظام الرقمي قيد النشاط، تحديد التهديدات ومصادرها، تحديد نقاط الضعف الموجودة في النظام الرقمي، القيام بعملية إختبار النظام الرقمي بواسطة التهديدات المحددة عبر نقاط الضعف المُكتشفة، تحديد الضوابط والوسائل الإدارية والتقنية للتحكم والسيطرة والحماية، تصنيف مستوى التهديدات واحتمالية التعرض لها وتحديد أثرها، التقييم النوعي والكمي للمخاطر، اقتراح التوصيات الضرورية للتحكم في المخاطر. (بن حسن العريشي و حسن الشلهوب، 2016، ص 57)، **والثانية هي الحد من المخاطر :**يتم في هذه العملية البدء في تنفيذ السياسة المُحددة للحد من المخاطر ويتم من خلالها اعتماد الأسلوب المناسب الذي يأخذ بعين الاعتبار التقليل في تكلفة استغلال موارد المنظمة ، ويتم في هذه العملية إتباع أربع إستراتيجيا ت(بن حسن العريشي و حسن الشلهوب، 2016، ص 76) محددة التكلفة وهي؛ التخفيف من أثر المخاطر من خلال تصحيح الخلل وسد الثغرات التي أحدثها التهديد والعمل على استمرار النظام الرقمي، نقل المخاطر من خلال إيجاد آلية تسمح بتحمل المخاطر نيابة عن النظام الرقمي المُستهدف كشركات التأمين مثلا، قُبول المخاطر وتعني السماح باستمرار عمل النظام الرقمي وسط تهديدات ومخاطر معروفة أو تلك المخاطر عالية التكلفة لتجنبها والتي لا تسبب خسائر كبيرة، تجنب المخاطر وتعني تفادي النشاطات والانخراط في أعمال يمكن أن تؤدي إلى حدوث مخاطر .

2.3. رصد الهجمات السيبرانية والتصدي لها: بعد اتخاذ الإجراءات الوقائية تأتي مرحلة الرصد والتصدي كعنصر مهم يضمن الإستجابة الفورية والفعالة بأي تهديد أو اختراق سيبراني محتمل وتتم من خلال:

- **أنظمة الرصد والتحليل:** الاعتماد على أنظمة كشف التسلل (IDS)وأنظمة منع التسلل (IPS) لرصد الأنشطة المشبوهة في الوقت الفعلي ، واستخدام الذكاء الاصطناعي وتحليل البيانات لتحديد الأنماط غير الاعتيادية التي قد تدل على وجود هجوم.
- **مراكز عمليات الأمن السيبراني (SOC):**تأسيس مراكز متخصصة لرصد الهجمات فور وقوعها ،والتعامل معها بشكل سريع وفعال ، و التعاون مع المنظمات الدولية والإقليمية في مجال تبادل المعلومات حول التهديدات السيبرانية الجديدة
- **استجابة فعاله للهجمات :** إعداد خطط واضحة ومحدده للتعامل مع الحوادث في السيبرانية بهدف تقليل أثارها المحتملة ، إستخدام نسخ احتياطيةآ مرة لاستعاد ة البيانات سريعا والحد من الخسائر الناجمة عن الهجمات.
- **اختبارات الاختراق:**تنفيذ اختبارات دوريةتحاكي الهجمات السيبرانية لتحديد الثغرات الأمنية المحتملة في الأنظمة، والعمل المستمر على تطوير حلول أمنية وتحديث الأنظمة لسد الفجوات الأمنية المكتشفة.

3.3. السيطرة على البيانات من اجل المحافظة على السيادة الرقمية : تشكل السيطرة على البيانات الوطنية الحجر الأساس للحفاظ على السيادة الرقمية وضمان إستقلالية القرارات المتعلقة بالموارد الرقمية الوطنية ، وتتم من خلال:

- **التحكم في مكان تخزين البيانات:** حفظ وتخزين البيانات الوطنية داخل حدود الدولة لتقليل الاعتماد على الخدمات السحابية الأجنبية، وإنشاء مراكز بيانات محليه لتعزيز السيطرة على البيانات وضمان أمانها.
- **تشريعات وسياسات حماية البيانات:** وضع قوانين وطني ة ملزمة تضمن حماية بيانات المُستخدمين والشركات، وتحديد سياسيات تنظيمية واضحة لعمليات نقل البيانات عبر الحدود الوطنية.
- **توطين التكنولوجيا وتعزيز الإبتكار:** دعم أنشطة البحث والتطوير التكنولوجي من اجل تحقيق اكتفاء ذاتي رقمي للدولة، وتشجيع الشركات المحلية على تطوير حلول تكنولوجيةمتقدمة تنافس الحلول الأجنبية.
- **التعاون الدولي وتعزيز الشراكات:** إبرام اتفاقيات تعاون دولية تساهم في حماية المصالح الوطنية فيما يتعلق بإدارة البيانات ، و المشاركة في شبكات ومنصات دولي ة لتبادل المعلومات والخبرات من اجل التصدي الجماعي للتهديدات السيبرانية.

الخاتمة :

حوكمة إدارة البيانات تمثل خط الدفاع الأول في مواجه ة الجرائم السيبرانية وحماية السيادة الرقمية حيث تُعتبر الضمان والأمان والفعالية من المخاطر الالكترونية ، وكذا في دعم حماية الأصول الرقمية للدول والمؤسسات وذلك عند تطبيق معايير الأمان اللازمة وتعزيز الالتزام بالقوانين الوطنية والدولية ، فحوكمة إدارة البيانات لها أهمية استراتيجيه بالغه بالتصدي للجرائم السيبرانية وضمان السيادة الرقمية للدول ، ذلك أن الوقاية الاستباقية من الجرائم الالكترونية وتطوير أنظمة الرصد والتحليل والاستجابة الفعالة وتعزيز السيطرة على البيانات تُمكن الدول من حماية أمنها الرقمي وتقليل التهديدات السيبرانية المحتملة ، كما أن صياغة التشريعات المناسبة وتوطين التقنيات الرقمية ودعم الابتكار المحلي يساهم بشكل كبير في تحقيق استقلالية القرار الوطني وتامين الموارد الرقمية ، وعليه فان التكامل بين الجهود المحلية والدولية في إدارة البيانات يُعتبر ضرورة حتمية لضمان استمرارية الأمن الرقمي والمحافظة على السيادة في العصر الرقمي المتغير المتسارع ، وعلى الرغم من النجاحات البارزة في تطبيق حوكمة إدارة البيانات في العديد من الدول ، مثل سنغافورة واستونيا إلا أن الدول النامية لا تزال تواجه تحديات كبرى من بينها ضُعف البُني التحتية التكنولوجية وغياب التشريعات الملائمة ونقص الكفاءات البشرية المتخصصة ، هذه التحديات تعيق بشكل كبير قدرته ا على التحكم في بياناتها الوطنية وتأمينها من التهديدات السيبرانية المتزايدة ، هذه الدول تقبع في دائرة التبعية التكنولوجية للشركات العالمية ويُعرض سيادتها الرقمية لمخاطر مستمرة .

ولأجل تجاوز التحديات التي تواجهها الدول النامية وتحقيق السيادة الرقمية بشكل حقيقي يُوصى بالتركيز على تطوير التشريعات الوطنية المتعلقة بحماية البيانات الشخصية والأمن السيبراني كما يجب الاستثمار في بناء بنية تحتية رقمية وطنية متطورة بالإضافة إلى إطلاق برامج تعليمية وتدريبي ة مكثفة لتأهيل كوادر متخصصة في إدارة البيانات وحمايتها وتعزيز التعاون الدولي لنقل الخبرات التقنية من الدول المتقدمة إليها بما يضمن تحقيق استقلال رقمي شامل ومستدام.

قائمة المراجع :

المراجع باللغة العربية :

جبريل بن حسن العريشي، و محمد حسن الشلهوب. (2016). *أمن المعلومات* (الطبعة الاولى). عمان: الدار المنهجية للنشر والتوزيع.

حسام رشيد هادي. (2023). *تأثير الذكاء الاصطناعي في النظام الدولي* (الطبعة الاولى). عمان: دار كفاءة المعرفة للنشر والتوزيع.

عبد الوهاب جعيجع. (2017). *الأمن المعلوماتي وإدارة العلاقات الدولية* (الطبعة الأولى). الجزائر: دار الخلدونية.

رغدة البهي. (03 07، 2022). *المركز المصري للفكر والدراسات الاستراتيجية*. تاريخ الاسترداد 17 03، 2025، من موقع المركز المصري للفكر والدراسات الاستراتيجية: https://ecss.com.eg/19881

عادل جربوعة، و عبد الجبار بوطمين. (12، 2023). الفضاء الرقمي والأمن السيبراني. *مجلة العلوم الانسانية* ، الصفحات 453-464.

عبد الغاني شرقي. (04 06، 2023). التهديدات السيبرانية وإشكالية السيادة : إعادة قرأة لسيادة واستفاليا. *مجلة السياسة العالمية* ، الصفحات 270-286.

فائزة مراد، و جيلالي شويرب. (20 04، 2023). مفهوم الجريمة السيبرانية والامن السبيراني . *مجلة الحقوق والحريات* ، الصفحات 157-178.

هايدي علي فهمي، و هبة يوسف هاشم. (04، 2024). الحوكمة الرشيدة والتنمية الاقتصادية : الفرص والتحديات (دراسة حالة للتجربة المصرية خلال الفترة 2002-2022). *المجلة الدولية للسياسات العامة في مصر* ، الصفحات 12-41.

محمد الشرشابي ،(23 ديسمبر 2025).السيادة الرقمية ..الوجه الجديد للسيادة الوطنية ، مركز الامن السبيراني للابحاث والدراسات ، الدوحة .

علي مال الله عبد الله، و خالص حسن الناصر. حوكمة امن المعلومات ودورها في تخفيض مخاطر نظم المعلومات المحاسبية الالكترونية. *حوكمة امن المعلومات ودورها في تخفيض مخاطر نظم المعلومات المحاسبية الالكترونية*، (الصفحات 1-9). نينوى.

الجزيرة الاخبارية. (18 07، 2018). الجزيرة الاخبارية. تاريخ الاسترداد 22 07، 2025، من موقع الجزيرة الاخبارية: https://www.aljazeera.net/blogs/2018/7/18

الجزيرة الاخبارية. (14 03، 2023). الجزيرة الاخبارية. تاريخ الاسترداد 23 07، 2025، من موقع الجزيرة الاخبارية: https://www.aljazeera.net/ebusiness/2023/3/14

نبيل عودة. (18 07، 2018). قناة الجزيرة الاخبارية. تاريخ الاسترداد 16 03، 2025، من موقع قناة الجزيرة الاخبارية: https://www.aljazeera.net/blogs/2018/7/18

الهيئة السعودية للبيانات والذكاء الاصطناعي(سدايا).(2021) .ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية. السياسات والضوابط-3

المراجع باللغة الأجنبية :

Abdulmajeed Abdulrahman, A., & Khalel Ibrahem, M. (2021, 01 30). Intrusion Detection System Using Data Stream Classification. *raqi Journal of Science* , pp. 319-328.

Bellanger, P., & Thida Norodom, A. (2023). Penser la transition numérique : Vers un monde digital durable Sous la direction de Matthieu Caron. *La souveraineté numérique* , pp. 41-50.

Diamond, J. (2020,). De l'inégalité parmi les sociétés Essai sur l'homme et l'environnement dans l'histoir. *Folio Essais* , pp. 391-437.

Diarra, G., & Plane, P. (2012). La Banque mondiale et la genèse de la notion de bonne. *Mondes en développement* , pp. 51-70.

Eraly, A., & goransson, M. (2021, 05). Gouvernance dans : Les nouveaux lieux communs de la droite. *La Revue Nouvelle* , pp. 43-48.

Ghernaouti, S. (2023). 10-Stratégie de lutte contre la cybercriminalité. *Cybercriminalité : Comprendre Prévenir Réagir* , pp. 223-251.

Rahman Mahmoud, A., & Madjid Hameed, S. (2023, 08 30). Review of Smishing Detection Via Machine Learning. *Iraqi Journal of Science* , pp. 4244-4259.

Türk, P. (2020, 09 14). Comprendre la souveraineté numérique. *Définition et enjeux de la souveraineté numérique* , pp. 18-28.

astra. (2025, 01 07). *astra*. Retrieved 03 20, 2025, from astra: https://www.astera.com/ar/type/blog/data-governance-best-practices/

Bradshaw, A. (2025, 10 22). *Alation*. Retrieved 11 20, 2025, from Alation: https://www.alation.com/blog/what-is-data-governance-policy/

Cimpanu, C. (2022, 02 16). *The Record*. Retrieved 07 26, 2025, from The Record: https://therecord.media/us-says-russian-hackers-breached-multiple-dod-contractors

Corera, G. (2021, 12 10). *BBC News*. Retrieved 07 26, 2025, from BBC News: https://www.bbc.com/news/technology-59612917.

Dellinger, A. J. (2021, 04 03). *Forbes*. Retrieved 07 23, 2025, from Forbes: https://www.forbes.com/sites/ajdellinger/2021/04/03/personal-date-of-533-million-facebook-users-leaks-online/

Desmarais, A. (2025, 02 27). *Euro News*. Retrieved 03 17, 2025, from Arabic Euro News: https://arabic.euronews.com/next/2025/02/28/reliance-us-tech-companies-threaten-europe-sovereignty-netherlands-google-cloud-data-trump

Government Technology Agency of Singapore (GovTech). (n.d.). *Government Technology Agency of Singapore (GovTech)*. Retrieved 03 16, 2025, from Government Technology Agency of Singapore (GovTech): www.tech.gov.sg

Hoskins, P. (2023, 01 18). *Bbc News*. Retrieved 07 19, 2025, from Bbc News: https://www.bbc.com/news/business-64313624

IBM . (2021). *Cost of a Data Breach Hits Record High During Pandemic.* CAMBRIDGE: newsroom ibm.

Kim, J., & Aravindan, A. (2018, 07 18). *Reuters*. Retrieved 07 22, 2025, from Reuters: https://www.reuters.com/article/world/uk/singapores-worst-cyberattack-steals-personal-data-of-15-million-including-pm-idUSKBN1KA14A/

Lyngaas, S. (2023, 07 12). *CNN Politics*. Retrieved 07 26, 2025, from CNN Politics: https://edition.cnn.com/2023/07/12/politics/china-based-hackers-us-government-email-intl-hnk

Nordic Institute for Interoperability Solutions. (n.d.). *X-Road*. Retrieved 03 16, 2025, from X-Road: www.x-road.global

Porter, A. (2024, 07 11). *bigid*. Retrieved 03 16, 2025, from bigid: https://bigid.com/blog/data-governance-policy-best-practices/

Reuters. (2022, 09 07). *Reuters*. Retrieved 07 27, 2025, from Reuters: https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/

Satish, B. (2018, 07 19). *Bbc News* . Retrieved 07 22, 2025, from Bbc News: https://www.bbc.com/news/world-asia-india-44856910

The Guardian. (2022, 01 14). *The Guardian*. Retrieved 07 26, 2025, from The Guardian: https://www.theguardian.com/world/2022/jan/14/ukraine-massive-cyber-attack-government-websites-suspected-russian-hackers.

Tidy, J. (2020, 07 27). *BBC News*. Retrieved 07 22, 2025, from BBC News: https://www.bbc.com/news/technology-53553576

Tidy, J. (2021, 07 19). *BBC News*. Retrieved 07 22, 2025, from BBC News: https://www.bbc.com/news/technology-57881364

Watson, J., & Images, G. (2021, 05 21). *CNET*. Retrieved 07 26, 2025, from CNET: https://www.cnet.com/news/privacy/colonial-pipeline-ceo-tells-senate-decision-to-pay-hackers-was-made-quickly/

European Union Agency for Cybersecurity (ENISA). (2020). *Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.*Athina : European Union Agency for Cybersecurity (ENISA).