جامعة غرداية

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

بالتعاون مع مخبر أبحاث البنية الرقمية والذكاء الاصطناعي وتطبيقاتهما في التحول الرقمي للقطاعات الاقتصادية.

وبالإشتراك مع فرقة بحث متطلبات تطبيق حوكمة الشركات والتدقيق المحاسبي في المؤسسات الإقتصادية الجزائرية بمخبر الدراسات التطبيقية في العلوم المالية.

وبالإشتراك مع النقابة الوطنية المستقلة لمستخدمي التعليم العالي - فرع غرداية، ينظمون:

الملتقى الوطني الأول (حضوري وعن بعد) حول: حوكمة مؤسسات التعليم العالي في ظل التحول الرقمي والتشريعات الحديثة.

مداخلة بعنوان:

الحوكمة الرقمية كإطار أخلاقي لتعزيز أمن المعلومات
Digital Governance as an Ethical Framework For Enhancing Information Security

من إعداد الباحثين :من خلال المحور رقم: 04 .

- **الإسم الكامل للباحث1،د.بهاز حمزة ، جامعة غرداية,** bahaz.hamza @univ-ghardaia.edu.dz
- **الإسم الكامل للباحث2، د.أولاد العيد بوحفص، جامعة غرداية ،** ouladlaid.bouhfs@univ-ghardaia.edu

الملخص:

تعد الحوكمة الرقمية من الركائز الأساسية التي تضمن استدامة المؤسسات في العصر الرقمي, حيث برزت كإطار تنظيمي لا غنى عنه لإدارة الموارد التكنولوجية وحمايتها, تسعى هذه الدراسة إلى استكشاف دور الحوكمة الرقمية كإطار استراتيجي لتعزيز أمن المعلومات, وذلك من خلال تحليل المفاهيم الجوهرية المرتبطة بهذين المجالين المترابطين.

يتم تحقيق أهداف الدراسة عبر تسليط الضوء على ماعية الحوكمة الرقمية, ثم الانتقال لتحليل أثرها المباشر في تحصين البيئة المعلوماتية ضد المخاطر السيبرانية, كما تتناول الدراسة ببحث أبحث التحديات والقيود التي تواجه المؤسسات عند تطبيق معايير الحوكمة, وصولا إلى الكشف عن أهم الآليات والمنهجيات التي تسهم في رفع كفاءة الأمن المعلوماتي تحت مظلة الحوكمة الرشيدة, وفي الختام نستعرض في هذه الدراسة جملة من الاستنتاجات

Abstract:

Digital governance is a fundamental pillar for ensuring organizational sustainability in the digital age, having emerged as an indispensable regulatory framework for managing and protecting technological resources. This study explores the role of digital governance as a strategic framework for enhancing information security by analyzing the core concepts associated with these two interconnected fields.

The study achieves its objectives by clarifying the nature of digital governance and analyzing its direct impact on fortifying the information environment against cyber risks. Furthermore, the research examines the prominent challenges and constraints organizations face when implementing governance standards. It concludes by identifying the key mechanisms and methodologies that contribute to elevating information security efficiency under the umbrella of sound governance. Finally, the study presents a set of conclusions and practical recommendations aimed at guiding organizations toward adopting integrated governance models that ensure the confidentiality and integrity of their data.

Keywords: Digital Governance, Information Security, Security Policy, Technical Challenges.

- مقدمة:

يشهد العالم المعاصر تسارعا غير مسبوق في وتيرة التحول الرقمي, حيث أصبحت التقنيات الحديثة ركيزة أساسية في مختلف مجالات الحياة الاقتصادية والاجتماعية والإدارية, وقد أدى هذا التحول إلى تعاظم حجم البيانات المتداولة واعتماد المؤسسات على الأنظمة الرقمية في إدارة عملياتها الحيوية.

وفي ظل هذا التطور, برز مفهوم الأمن المعلوماتي كأحد التحديات الكبرى, نظرا لتزايد المخاطر السيبرانية التي تهدد سرية المعلومات وسلامتها وتوافرها, إذ لم يعد التعامل مع هذه التهديات قاصرا على الحلول التقنية البحتة, بل تطلب مقاربات شاملة تجمع بين الجوانب التنظيمية والقانونية والأخلاقية. ومن هنا أصبح تأمين المعلومات ضرورة استراتيجية لضمان استمرارية الأعمال وحمية الأصول الرقمية من الاختراقات والهجمات الالكترونية.

غير أن تحقيق الأمن المعلوماتي لايقتصر على الجوانب التقنية فقط بل يتطلب إطارا تنظيميا يضمن الاستخدام الرشيد والمسؤول للتكنولوجيا.

وفي هذا السياق, ظهرت الحوكمة كآلية لإرساء مبادئ الشفافية والمساءلة والرقابة في إدارة الموارد والعمليات داخل المؤسسات, إذ تسعى إلى تحقيق التوازن بين مختلف الأطراف المعنية وضمان اتخاذ قرارات فعالة ومسؤولة ومع تطور البيئة الرقمية تطور مفهوم الحوكمة ليشمل المجال الرقمي, فيما يعرف بالحوكمة الرقمية والتي تختص بتنظيم الفضاء الرقمي وإدارة الأصول المعلوماتية ضمن بيئة تكنولوجية معقدة ومترابطة بما يتماشى مع الأهداف الاستراتيجية للمؤسسات.

كما تهدف إلى وضع سياسات ومعايير تضمن الاستخدام الآمن والأخلاقي للأنظمة المعلوماتية.

وفي هذا الإطار تبرز الحوكمة الرقمية كمرجعية أخلاقية توجه ممارسات الأمن المعلوماتي وتحدد ضوابطه, كما أنه تسهم في تعزيز الثقة الرقمية من خلال ترسيخ مبادئ النزاهة والمسؤولية في التعامل مع البيانات واحترام خصوصية الأفراد.

وعليه تعد الحوكمة الرقمية إطارا أخلاقيا متكاملا لتعزيز أمن المعلومات, بما يضمن حماية البانات وتحقيق الاستخدام المستدام والآمن للتقنيات الحديثة.

وبناء على ذلك تعالج هذه الدراسة الاشكالية الرئيسية المتمثلة في:

إلى أي مدى تساهم الحوكمة الرقمية كإطار أخلاقي في تعزيز امن المعلومات وحماية البيانات داخل المؤسسات؟ وذلك من خلال التوقف عند مفهوم الحوكمة الرقمية وعلاقتها بالأخلاقيات الرقمية, وتحليل تأثير مبادئها على أمن المعلومات, ورصد التحديات التي تعترض تطبيقها, واقتراح الآليات الممكنة لتعزيز الأمن المعلوماتي من خلالها, أين يتم الإلمام بهذا الطرح من خلال التساؤلات التالية:

1- ما المقصود بالحوكمة الرقمية وما علاقتها بالأخلاقيات الرقمية؟
2- كيف تؤثر مبادئ الحوكمة على أمن المعلومات؟
3- ما أهم التحديات التي تواجه تطبيق الحوكمة الرقمية؟
4- ما الآليات الممكنة لتعزيز الأمن المعلوماتي من خلال بالحوكمة الرقمية؟

أولا: أهداف الدراسة:

- تهدف الدراسة الحالية إلى جملة من الأهداف نسردها فيما يلي:
- تسليط الضوء على أهم المفاهيم حول الحوكمة الرقمية.
- التعرف إلى تأثير الحوكمة على أمن المعلومات.
- التعرض لأبرز التحديات والقيود التحديات التي تواجه تطبيق الحوكمة الرقمية.
- الكشف عن أهم الآليات الممكنة لتعزيز الأمن المعلوماتي من خلال بالحوكمة الرقمية.

ثانيا:أهمية الدراسة:

-الإلمام بواقع الحوكمة الرقمية وعلاقتها بالأخلاقيات الرقمية وأمن المعلومات عن طريق إعطاء نظرة مفصلة حول هذا المفهوم .
- الاطلاع على أفضل الممارسات التي تظهر تطبيق الحوكمة الرقمية كإطار اخلاقي في تعزيز الأمن المعلوماتي .
- الاطلاع على أهم التحديات والفرص التي تواجه المؤسسات, والمساعدة في تقديم رؤى قيمة للمؤسسات التي تفكر في تبني أخلاقيات الحوكمة الرقمية في تعزيز الأمن المعلوماتي .

ثالثا:الإطار النظري للدراسة:

1-مفهوم الحوكمة الرقمية:

يشير مصطلح الحوكمة الرقمية إلى استخدام التقنيات الرقمية والبيانات والأطر التنظيمية لتحسين عملية صنع القرار والشفافية والمساءلة داخل المؤسسات,

ويشمل ذلك السياسات والإجراءات والهياكل التي توجه كيفية إدارة الموارد الرقمية والتحكم بها. وفي العصر الحديث، تلعب الحوكمة الرقمية دورا محوريا في تعزيز تقديم الخدمات وبناء الثقة بين المؤسسات وأصحاب المصلحة. علاوة على ذلك، تدمج الحوكمة الرقمية الفعالة المبادئ الأخلاقية والتدابير الأمنية لضمان الاستخدام المسؤول والآمن لأنظمة المعلومات.

1-1-تعريف الحوكمة الرقمية:

الحوكمة الرقمية هي إطار عمل لتحديد المساءلة والأدوار وسلطة اتخاذ القرار فيما يتعلق بالحضور الرقمي للمؤسسة، والذي يشمل مواقعها الإلكترونيـة، ومواقعها على الأجهزة المحمولة، وقنوات التواصل الاجتماعي، وأي منتجات وخدمات أخرى مرتبطة بالإنترنت والويب, كما أن إطار الحوكمة الرقمية هو نظام يفوض سلطة اتخاذ القرارات الرقمية المتعلقة بمنتجات وخدمات رقمية محددة من صلب المؤسسة إلى أقسام أخرى فيها.(Dogou, 2025)

عندما يتم التحدث عن الحوكمة الرقمية، فإنه يشار إلى القواعد المتعلقة باستخدام الوسائل التكنولوجية الرقمية في البنية التحتية للمعلومات, حيث يمكن للاختيارات التي يتخذها مصممو الأنظمة وصناع السياسات بشأن بنية نظم المعلومات والمعايير التقنية أن تؤثر بشكل كبير على كيفية دمج التقنيات الرقمية في عمليات الحوكمة العامة, غالبا ما تنطوي هذه القرارات على مفاضلات بين تعزيز القدرات في عمليات الحوكمة العامة وتأثير خيارات التصميم على الثقافة التنظيمية والإجراءات الإدارية ونتائج السياسات.(Grigalashvili, 2023).

كما تفهم الحوكمة الرقمية على أنها إطار تنظيمي يعتمد على التقنيات الرقمية الحديثة مثل الخوارزميات والذكاء الاصطناعي والبلوكتشين, يهدف هذا الإطار إلى إدارة عمليات التحكم والتنسيق بين الأفراد والمؤسسات داخل البيئات الرقمية المعقدة.(Hanisch, Goldsby, Fabian, & Oehmichen, 2023)

فيما يشير تعريف آخر لمصطلح الموكمة الرقمية إلى أنها شكل من اشكال التنظيم الذي يستفيد من التقنيات الرقمية,مثل الخوارزميات والذكاء الاصطناعي وتقنية سلسلة الكتل (البلوك تشين), لإدارة الرقابة والتنسيق والحوافز والثقة في علاقات التبادل الرقمية.(Matei & Bujac, 2016)

من خلال ماسبق نستطيع أن نقول أن الحوكمة الرقمية هي إطار عمل يحدد الأدوار والمسؤوليات وسلطة اتخاذ القرار المتعلقة بالحضور الرقمي للمؤسسة مثل المواقع الالكترونية والتطبيقات ووسائل التواصل الاجتماعي, كما تقوم على تفويض القرارات الرقمية إلى الجهات المختصة داخل المؤسسة دون التدخل في عمليات الإنتاج أو استراتيجيات المحتوى أو البنية المعلوماتية. وهي كذلك قواعد تنظم استخدام التقنيات الرقمية داخل أنظمة المعلومات مع مراعاة التوازن بين الكفاءة التشغيلية والتكاليف التنظيمية, أين تعتمد على تقنيات حديثة مثل الذكاء الاصطناعي والبلوكتشين والخوارزميات لتنظيم التحكم والتنسيق والثقة في البيئات الرقمية.

2-1-مبادئ الحوكمة الرقمية:

تبنى الحوكمة الرقمية الفعالة على أساس مبادئ جوهرية تضمن تسخير التكنولوجيا لخدمة المصلحة العامة مع الحفاظ على نزاهة المؤسسات. ومن أهم عناصر هذا الإطار الشفافية والمساءلة وحماية البيانات، التي تعزز مجتمعة الثقة بين الدولة ومواطنيها, ومن خلال دمج هذه القيم في البنية التحتية الرقمية، تستطيع الحكومات الانتقال من النماذج البيروقراطية التقليدية إلى أنظمة أكثر انفتاحا وأمانا واستجابة.

2-1-أ-الشفافية:

تعد الشفافية أحد العناصر الأساسية للحوكمة الرقمية، حيث تستخدم الحكومة التكنولوجيا لإتاحة المعلومات للجمهور على نطاق واسع, ومن خلال استخدام منصة الحكومة الإلكترونية، تستطيع الحكومة تقديم خدمات عامة أسرع وأكثر كفاءة، مع تعزيز مشاركة الجمهور في صنع القرار, وقد ذكر بيرتوت، وجيجر، وغرايمز (2010) أن تطبيق التكنولوجيا الرقمية في الحكومة يمتلك إمكانات هائلة للحد من ممارسات الفساد، وزيادة المساءلة، وبناء ثقة الجمهور.(Paselle, Indarto, & Rande, 2025)

2-1-ب-المساءلة:

من أبرز مزايا تطبيق الحكومة الإلكترونية زيادة الشفافية والمساءلة في الإدارة العامة, فبفضل المنصات الرقمية، أصبح الوصول إلى المعلومات التي كان يصعب على الجمهور الوصول إليها سابقا أمرا يسيرا, فعلى سبيل المثال، بات بالإمكان

نشر ميزانيات الحكومة وسياساتها العامة وتقاريرها المالية إلكترونيا، مما يتيح للجمهور مراقبة وتقييم أداء الحكومة بشكل أكثر فعالية.(Setyarto, Alimuddin, Mulyaningsih, & Judijanto, 2025)

2-1-ج- حماية البيانات:

تحمي حماية الخصوصية في الحكومة الرقمية المعلومات الشخصية للمواطنين وأمن بياناتهم الشخصية أثناء إفصاح الحكومة عن المعلومات, وتعد حمايـة الخصوصية مفهوما متعدد الأوجه يمنع إساءة استخدام البيانات الشخصية أو تسريبها أو الوصول إليها بشكل غير مصرح به، مع ضمان استخدامها في بيئة قانونية وشفافة وخاضعة للرقابة, ولتحقيق هذا الهدف، لا بد من اتخاذ تدابير، تشمل تحسين القوانين ذات الصلة، وتطبيق إجراءات أمنية تقنية صارمة، وتوضيح حدود استخدام البيانات.(Chen, 2024)

2-مفهوم الأمن المعلوماتي:

في ظل التطور الرقمي المتسارع واعتماد المؤسسات والأفراد على الأنظمة المعلوماتية, أصبح الحفاظ على البيانات وحمايتها من المخاطر أمرا ضروريا لا غنى عنه, حيث يعد الأمن المعلوماتي أحد المفاهيم الأساسية التي تهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها, كما يشمل مجموعة من الإجراءات والتقنيات والسياسات التي تحمي الأنظمة من الاختراق أو الفقدان أو التلاعب, ومن هذا المنطلق يبرز الأمن المعلوماتي كعنصر حيوي في تعزيز الثقة في البيئة الرقمية وضمان استمراريتها , وسنستعرض فيما يلي مجموعة من التعاريف العلمية التي تناولت هذا المصطلح من زوايا مختلفة وكذا عناصر الأمن المعلوماتي:

2-1-تعريف أمن المعلومات:

أمن المعلومات هو حماية المعلومات وعناصرها الحيوية، بما في ذلك الأنظمة والأجهزة التي تستخدم هذه المعلومات وتخزنها وتنقلها, ويشمل ذلك حماية أصول المعلومات من التهديدات ونقاط الضعف والحوادث الضارة المحتملة التي قد تؤثر على المؤسسة, حيث يكمن الهدف الرئيسي في ضمان سرية المعلومات وسلامتها وتوافرها.(Brunner, Sauerwein, Felderer, & Breu, 2020)

فيما ذكر تعريف آخر بكونه نظام حوكمة وإدارة يضمن حماية أصول المعلومات من خلال ضوابط تقنية وتنظيمية وإدارية منسقة, ويهدف إلى الحفاظ على سرية

البيانات وسلامتها وتوافرها داخل المؤسسة، مع منع الوصول غير المصرح به إليها أو إساءة استخدامها أو فقدانها, كما يشمل تطبيق تدابير أمنية تتراوح بين الأنظمة التقنية وسياسات الإدارة وأطر حوكمة المخاطر.(Ohki, Harada, Kawaguchi, Shiozaki, & Kagaya, 2009)

أما كورهونين وآخرون(Korhonen et al) عرفوه على أنه تخصص يعنى بحماية المعلومات وعناصرها الحيوية، بما في ذلك الأنظمة والأجهزة المستخدمة لتخزينها ومعالجتها ونقلها, ويهدف إلى ضمان سرية المعلومات وسلامتها وتوافرها داخل المؤسس, .ويشمل ضوابط فنية وإدارية وتشغيلية تحمي أصول المعلومات من الوصـول غـير المصـرح بـه أو سـوء الاسـتخدام أو الفقـدان.(Korhonen, Hiekkanen, & Mykkänen, 2012)

2-2-عناصر أمن المعلومات:

يكمن جوهر أي استراتيجية دفاعية قوية في إطار عمل مصمم لحماية البيانات من التهديدات المتغيرة باستمرار. تعرف هذه الركائز الثلاث باسم "ثالوث CIA"، وهي: السرية، والسلامة، والتوافر، وتشكل الأساس الجوهري لأي بيئة آمنة. ومن خلال تحقيق التوازن بين هذه العناصر، تضمن المؤسسات بقاء المعلومات الحساسة سرية ودقيقة ومتاحة لمن يحتاجون إليها.

2-2-أ-السرية:

تعرف السرية بأنها القيود المفروضة على استخدام وتخزين أنواع البيانات المختلفة لمنع الكشف غير المصرح به, وهي توفر آلية لصلاحية فك تشفير مرنة من خلال توليد مجموعات مفاتيح لا تتأثر بالعدد الإجمالي للمفاتيح المشفرة. تشمل الأساليب الحديثة أيضا المصـادقة الواعيـة بالخصوصـية لإدارة النمـو الهائـل لمستخدمي الشبكة مع الحفاظ على نقل البيانات بشكل آمن.(Yee & Zolkipli, 2021)

2-2-ب-السلامة:

تستخدم آليات الأمان لضمان سرية جميع معلومات المستخدمين المُستعان بمصادر خارجية، مثل البيانات والهوية الشخصية والموقع، حتى في مواجهة جهات خصوم نزيهة ولكنها فضولية. إضافة إلى ذلك، تسهم آليات أمان البيانات، كالتشفير

ومراجعة سلامة البيانات والمصادقة والتحكم في الوصول، في الحفاظ على خصوصية المستخدمين بشكل مباشر أو غير مباشر في الحوسبة الطرفية. تضمن هذه الإجراءات الحفاظ على سرية البيانات وسلامتها حتى عند فصل ملكية البيانات عن التحكم فيها.(Zhang, Chen, Zhao, Cheng, & Hu, 2018)

2-2-ج-التوافر:

موثوقية نظام الحوسبة السحابية. في هذا المجال، يعد تحسين التنبؤ بسعة الشبكة تحديا رئيسيا، نظرا لجهل مستوى الإدارة غالبا بتوافر الموارد, حيث تشارك الموارد المتاحة والمؤتمتة عادة بين العديد من العملاء، مما قد يؤدي، للأسف، إلى الوصول غير المصرح به إلى بياناتهم. علاوة على ذلك، تستهدف الهجمات الأمنية الشائعة، مثل هجمات حجب الخدمة (DoS)، توافر النظام بشـكل مباشـر. (Shabbir et al., 2024)

3- العلاقة بين الحوكمة الرقمية وأمن المعلومات:

ترتبط الحوكمة الرقمية وأمن المعلومات ارتباطا وثيقا من خلال التزام مشترك بالحفاظ على الثقة النظامية والمرونة التشغيلية. ويكمن جوهر هذه العلاقة في دور القيم الأخلاقية، التي توجه ممارسات حماية البيانات بما يتجاوز مجرد الامتثال القانوني لضمان المعاملة العادلة والشفافة لمعلومات المستخدمين, ويخلق تكامل هذين الجانبين إطارا متماسكا تعمل فيه الرقابة الاستراتيجية والضوابط التقنية بتناغم للحد من المخاطر.

3-1- دور القيم الأخلاقية في حماية البيانات:

تتطلب حماية البيانات الشخصية في العصر الرقمي نهجا أوسع يدمج المبادئ الأخلاقية المتعلقة بالعدالة الاجتماعية والإنصاف والشفافية, حيث لم يعد بالإمكان تصور حماية البيانات الفعالة من منظور الامتثال القانوني فحسب، بل تستلزم إطارا قائما على القيم لتوجيه الابتكار التكنولوجي نحو الصالح العام. أخلاقيا، ينطوي احترام المساءلة على التزام حقيقي باستقلالية الفرد وكرامته، بما يضمن قدرة الأفراد على التصرف والتواصل دون قيود غير مبررة.(Buruiana, 2025)

3-2- التكامل بين الجانبين:

يمثل دمج التقنيات المتقدمة، كالذكاء الاصطناعي، في أنظمة أمن المعلومات تحولا جذريا في كيفية إدارة أطر الحوكمة الرقمية للأمن السيبراني , ويمثل هذا

التقارب نقلة نوعية، إذ يسمح للحكومات بالانتقال من البروتوكولات التفاعلية إلى استراتيجيات استباقية مدعومة بالذكاء الاصطناعي، لحماية الخدمات العامـة وضمان استمرارية الوظائف الحيوية. ومن خلال الاستفادة من التعلم الآلي لتحديد الأنماط الشاذة والتنبؤ بنقاط الضعف، تعزز هذه الأنظمة المتكاملة البنى التحتية الرقمية في مواجهة التهديدات المتزايدة التعقيد.(Muhammad, Abas, Ahmad, & Sulaiman, 2024)

4- دور الحوكمة الرقمية في تعزيز أمن المعلومات

تشكل الحوكمة الرقمية الإطار الاستراتيجي الذي يواءم السياسات المؤسسية مع المتطلبات المتغيرة للمشهد السيبراني, ومن خلال وضع بروتوكولات واضحة وتحديد المساءلة، تحول الحوكمة الرقمية التدابير التقنية التفاعلية إلى ثقافة استباقية شاملة للمؤسسة تعزز المرونة, ويعد هذا الإشراف الهيكلي ضروريا لحماية البيانات الحساسة من التهديدات العالمية المتطورة باستمرار.

4-1- آليات الحوكمة في حماية المعلومات

تعتمد حماية المعلومات الفعالة على سياسات رقمية متينة تحدد الحدود الأخلاقية والتشغيلية لاستخدام البيانات. ومن خلال إدارة المخاطر المنهجية، تستطيع المؤسسات توقع نقاط الضعف وتحديد أولويات الموارد للتخفيف من الاختراقات المحتملة. وتعزز هذه الجهود بضوابط داخلية توفر المراقبة والتدقيق المستمرين اللازمين لضمان الامتثال, وتشكل هذه الآليات مجتمعة إطار حوكمة شاملا يحول الأمن من عقبة تقنية إلى رصيد استراتيجي.

4-1-أ- السياسة الرقمية:

تشكل السياسة الرقمية آلية حوكمة أساسية، إذ تحدد الأهداف الاستراتيجية والمبادئ والتوجيهات الأخلاقية لإدارة أصول المعلومات في المؤسسة, كما ترسخ "إطار السياسة" الرسمي الذي يحدد كيفية جمع البيانات وتصنيفها وحمايتها طوال دورة حياتها لضمان سريتها وسلامتها, ومن خلال وضع قواعد واضحة للتحكم في الوصول والامتثال التنظيمي، توفر هذه السياسات خارطة طريق تواءم سلوك الموظفين مع أهداف الأمن, فهي تحول السياسة الرقمية الاحتياجات الأمنية النظرية إلى توجيهات عملية، ما يسهم في سد الفجوة بين الحوكمة العليا والتنفيذ التقني.(Kehinde, 2025)

4-1-ب- إدارة المخاطر:

في سياق التحول الرقمي، تعمل إدارة المخاطر كآلية حوكمة متطورة من خلال إضفاء الطابع المؤسسي على تصنيف الضوابط وتطبيقها ومراقبتها المستمرة عبر أطر عمل مثل NIST SP 800-37 وISO 31000. ينتقل هذا النهج الأكاديمي الدقيق من التقييمات اليدوية الثابتة إلى منهجية تعتمد على القياس عن بعد، حيث تقاس المخاطر باستخدام مقاييس كمية مثل متوسط الخسارة المتوقعة (SLE) ومتوسط الخسارة المتوقعة السنوية (ALE), ومن خلال دمج هذه الأولويات القائمة على المخاطر مع مؤشرات مستوى الخدمة التشغيلية، مثل متوسط وقت الكشف والاستجابة، تستطيع المؤسسات تجاوز مجرد الامتثال لقوائم التحقق نحو نموذج ضمان تكيفي.(Malik, 2025)

4-1-ج- الرقابة الداخلية:

الرقابة الداخلية آلية حوكمة توفر آليات الرقابة والتوازن اللازمة لضمان تنفيذ إجراءات أمن المعلومات وفقا لتوجيهات مجلس الإدارة والإدارة العليا, وبعيدا عن مجرد التنفيذ التقني، تعمل هذه الرقابة كنظام إشراف شامل يتضمن توجيه الاستراتيجيات ومراقبة الأداء عبر مختلف المستويات التنظيمية الرسمية والتقنية وغير الرسمية, وباستخدام أطر عمل مثل نظرية الردع العام - التي ترتب الإجراءات من خلال الردع والوقاية والكشف والمعالجة - تقلل الضوابط الداخلية بشكل فعال من الاحتيال والهدر والمعاملات غير المصرح بها, حيث تحول هذه الآليات معايير الأمان السلبية إلى عملية مساءلة فعالة.(Musa, 2018)

4-2-البعد الأخلاقي لحماية البيانات

يتجاوز البعد الأخلاقي لحماية البيانات مجرد الامتثال القانوني، إذ يركز على المسؤولية الأخلاقية في احترام خصوصية الأفراد وكرامتهم الإنسانية, بما يضمن حماية استقلالية الأفراد في ظل بيئة رقمية متزايدة التطفل, حيث يتطلب ذلك التزاما بالاستخدام المسؤول للبيانات، حيث تخضع عملية جمـع المعلومـات ومعالجتها لمبادئ العدالة والشفافية وتحديد الغرض.

4-2-ا- احترام الخصوصية:

في الخطاب الأخلاقي المعاصر، يعرف احترام الخصوصية من خلال منظورين: الوصول والتحكم، حيث تمثل الخصوصية القدرة الأخلاقية للفرد على منح أو رفض

الوصول إلى نفسه أو معلوماته الشخصية. ويطبق هذا المفهوم عمليا عبر ثلاثة أبعاد أساسية: البعد المحلي (المكان المادي والجسد)، والبعد المعلوماتي (التحكم في معرفة البيانات الشخصية)، والبعد القراري (الحماية من التدخل غير المرغوب فيه في الخيارات الشخصية), وباعتبار الخصوصية عنصرا أساسيا في كرامة الإنسان واستقلاليته الشخصية، تضمن أطر الحوكمة قدرة الأفراد على الحفاظ على "شخصية مصونة" واستكشاف أدوار اجتماعية إبداعية دون الآثار السلبية للتدقيق المستمر.(Sax, 2018)

4-2-ب- الاستخدام المسؤول للبيانات:

يعرف الاستخدام المسؤول للبيانات ضمن البعد الأخلاقي لحماية البيانات بضرورة أساسية تتمثل في ضمان متانة منهجيات البحث مع العمل بفعالية على منع إلحاق الضرر أو المعاناة أو الوصم بصاحب البيانات, ووفقا للنص، يتجاوز هذا مجرد الامتثال القانوني، إذ يؤطر التعامل مع البيانات كمسؤولية أخلاقية للباحث لضمان أن تخدم النتائج "الصالح العام" وتحافظ على ثقة المجتمع, حيث يتضمن ذلك على وجه العمق، ضوابط صارمة للكشف لمنع الكشف عن "الهويـة" و"الخصائص"، حيث يتم الكشف عن معلومات حساسة مثل الحالة الصحية النفسية أو استنتاجها, كما يتطلب الاستخدام الأخلاقي الدقيق تقييما استباقيا "لمخاطر الكشف"، لضمان عدم إمكانية إعادة بناء البيانات الضخمة، حتى تلك التي تبدو مجهولة المصدر.(Wiltshire & Alvanides, 2022)

4-3- التحديات

يكشف استعراض مجال أمن المعلومات عن فجوة حوكمة حرجة، حيث تعجز السياسات والاستعداد البشري عن مواكبة التحولات التكنولوجية, ويعود هذا النقص في المقام الأول إلى ضعف الوعي الرقمي لدى المستخدمين، والافتقار المستمر إلى تشريعات حديثة لتنظيم الفضاءات الرقمية العابرة للحدود, علاوة على ذلك، يشكل التطور السريع للهجمات الإلكترونية هدفا متحركا، مما يجعل استراتيجيات الدفاع التقليدية بالية، ويستدعي إطار حوكمة أكثر مرونة , وفيما يلي أهم التحديات التي تواجه دور الحوكمة الرقمية في تعزيز أمن المعلومات:

4-3-أ- ضعف الوعي الرقمي:

يعد ضعف الوعي الرقمي، الذي يعرف بأنه "العامل البشري" أو نقص المعرفة الرقمية الأساسية، عائقا رئيسيا أمام نجاح الحوكمة الرقمية وأمن المعلومات, ويشمل ذلك عجز الفرد عن التقييم النقدي للمعلومات، أو إدراك المخاطر الأمنية، أو إدارة الهويات الرقمية، مما يجعل المستخدمين في كثير من الأحيان "الحلقة الأضعف" في أنظمة الحكومة الإلكترونية. فبدون وعي رقمي قوي، حتى الدفاعات التقنية المتطورة تفشل، حيث يتجاوز أصحاب المصلحة البروتوكولات دون علمهم أو يقعون ضحية للهندسة الاجتماعية وعمليات التصـيد الاحتيـالي.(Isabella, Agustian, Baharuddin, Ibrahim, & Regulation, 2025)

4-3-ب- نقص التشريعات:

غياب التشريعات الشاملة يشكل عائقا رئيسيا أمام الحوكمة الرقمية الفعالة، إذ غالبا ما يؤدي التطور السريع للتحول الرقمي إلى ظهور ثغرات لا تستطيع الأنظمة البيروقراطية والتنظيمية التقليدية معالجتها, وتتجلى هذه "الفجوة التنظيمية" في سياسات مجزأة وآليات إنفاذ ضعيفة، ما يحول دون مواءمة المؤسسات العامة لمبادراتها الرقمية مع المعايير القانونية اللازمة ومتطلبات حماية البيانات, وبدون أطر تشريعية متينة، يبقى الأمن السيبراني وظيفة تقنية معزولة بدلا من كونه مطلبا استراتيجيا للحوكمة، ما يجعل البنية التحتية الحيوية عرضة لثغرات منهجية. علاوة على ذلك، يُعيق غياب نماذج تنظيمية مُصممة خصيصًا لواقع القطاع العام قدرة صانعي السياسات على ترسيخ المرونة وضمان المساءلة أثناء الاضطرابات السيبرانية. وبالتالي، يعد الربط بين الابتكار التكنولوجي وابتكار السياسات أمرا بالغ الأهمية للحفاظ على شرعية الخدمات الرقمية وحماية ثقة الجمهور في بيئة متقلبة بشكل متزايد.(Aryanti, 2025)

4-3-ج- التطور السريع للهجمات السيبرانية:

يمثل التطور السريع للهجمات الإلكترونية تحديا بالغ الأهمية للمراقبة الرقمية والتحكم في أمن المعلومات، إذ أن تزايد الرقمنة يجعل العمليات الحكومية أكثر عرضة للوصول غير المصرح به والتعطيل, ولمعالجة هذه الثغرات، يعرف الأمن السيبراني بأنه الممارسة الأساسية لحماية الأصول الرقمية والبنية التحتية العامة من الهجمات المعقدة التي تستهدف البيانات الحساسة وتهدد الأمن القومي.(C.V, 2024)

5- سبل تعزيز الحوكمة الرقمية لأمن المعلومات

لضمان دفاع قوي ضد التهديدات السيبرانية المتطورة، يجب على المؤسسات تجاوز مجرد الامتثال الأساسي ودمج الأمن في صميم اسـتراتيجيتها. تركـز الاستراتيجيات التالية على مواءمة الضوابط التقنية مع الإشراف البشري لإنشاء بيئة رقمية مرنة, ومن خلال تحسين أطر السياسات والاستفادة من الإشراف الآلي، يستطيع القادة التخفيف من المخاطر بشكل استباقي قبل أن تتحول إلى اختراقات خطيرة.

5-1-الحلول التقنية

يعتمد أمن المعلومات الفعال على استراتيجية دفاع متعددة الطبقات تعطي الأولوية لسلامة وسرية البيانات الحساسة, ومن خلال نشر أنظمة حماية متطورة، تستطيع المؤسسات إنشاء محيط أمني يراقب ويصد أي وصول غير مصرح به في الوقت الفعلي, كما تضمن بروتوكولات التشفير القوية أنه حتى في حال اعتراض البيانات، تظل غير قابلة للقراءة وآمنة من الاستغلال.

5-1-أ- أنظمة الحماية والتشفير:

تنشئ أنظمة الحماية، مثل أمن الشبكات والبنية التحتية للحكومة الإلكترونية، دفاعا منهجيا عن أصول المعلومات الحيوية، مما يضمن مرونتها في مواجهة الوصول غير المصرح به والهجمات الإلكترونية المعقدة, حيث يعد التشفير عنصرا تقنيا أساسيا ضمن عناصر السرية والنزاهة وإمكانية الوصول، موفرا وسيلة قانونية ووظيفية لتلبية متطلبات الأطر القانونية لحوكمة الأمن خاصة في الاتحاد الأوروبي، مثل اللائحة العامة لحماية البيانات (GDPR) وأمن الشبكات والمعلومات (NIS), وباعتبارها وسيلة للحوكمة، لا تعد هذه الأدوات التقنية مجرد ميزات معزولة، بل تدمج في أطر حوكمة موحدة (مثل ISO/IEC 27001) لمواءمة أمن تكنولوجيا المعلومات مع استراتيجية المؤسسة وإدارة أدائها.(Magnusson, Iqbal, Elm, & Dalipi, 2025)

5-1-ب- الأمن السيبراني:

تعيد الدراسات الحديثة صياغة مفهوم الأمن السيبراني من مجرد "رقابة تشغيلية" هامشية إلى "بنية حوكمة" أساسية، معرفة إياه كمسؤولية تنفيذية استراتيجية تدمج الضمانات التقنية مع إدارة المخاطر على مستوى المؤسسة,

وكحل تقني، يشمل هذا المفهوم "الضوابط الوقائية" و"البنى التحتية المرنة" المصممة لحماية البيانات الحساسة والمنصات الشبكية، إلا أن فعاليته كوسيلة للحوكمة تعتمد على تحديد القادة التنفيذيين "مستوى تقبّل المخاطر" ومواءمة الأمن مع رسالة المؤسسة.(Zul Afida Abdullah., 2026)

2-5-الحلول التنظيمية

لضمان دعم الدفاعات التقنية بأساس قانوني متين، يتعين على المؤسسات تطبيق حلول تنظيمية شاملة تحدد نطاق الاستخدام المقبول وإدارة البيانات, تستند هذه التدابير إلى قوانين ولوائح صارمة توفر إطارا إلزاميا للامتثال والمساءلة في مختلف الإجراءات القضائية, كما تترجم هذه التوجيهات داخليا إلى سياسات فعالة داخل المؤسسات، مما يرسي خارطة طريق واضحة لسلوك الموظفين ومسؤولياتهم الإدارية. تحول هذه العناصر مجتمعة الأمن من هدف تقني إلى معيار حوكمة منظم وقابل للتنفيذ قانونا.

2-5-أ- قوانين وتشريعات صارمة:

القوانين واللوائح الصارمة هي تفويضات قانونية رسمية، خاصة بكل نظام سياسي، توفر مسارا ضروريا للسيطرة على العواقب غير المقصودة للتقنيات الناشئة والبيانات الضخمة, وكحل تنظيمي، تحول هذه القوانين واللوائح أمن المعلومات من مهمة تقنية "مؤقتة" إلى بنية حوكمة مهيكلة، مما يتطلب من فرق التصميم دمج "أفكار القوانين وصناع السياسات" مباشرة في البنى التحتية للحوسبة لمنع المؤسسات من استغلال ثغرات خصوصية العملاء.(Naidu & Chakravarthy, 2021)

2-5-ب- سياسات داخل مؤسسات:

سياسات أمن المعلومات (ISPs) هي بنية حوكمة رسمية تحدد الأدوار والمسؤوليات والقواعد وإجراءات التشغيل القياسية لحماية سرية وسلامة وتوافر الأصول الرقمية, وباعتبارها حلا تنظيميا أساسيا، تعمل سياسات أمن المعلومات كدليل هيكلي لمواجهة التهديدات الأمنية، وتحديد نقاط الضعف، واكتشاف الأخطاء البشرية، مما يحول التوجيهات التنفيذية إلى سلوكيات امتثال قابلة للتنفيذ, وإلى جانب التحكم التقني، تعمل هذه السياسات كوسيلة للحوكمة من خلال إنشاء إطار

عمل هرمي غالبا عبر التحكم في الوصول القائم على الأدوار (RBAC). (Sharma, Koohang, & Singh, 2025)

-خاتمة

ترسخ الحوكمة الرقمية إطارا شاملا ينسق بين الدفاعات التقنية والإشراف التنظيمي لحماية أهم أصول المؤسسة, وبالنظر إلى الحلول وأساليب الحوكمة التي تم استعراضها في هذه الدراسة، تشكل النتائج الرئيسية التالية خارطة طريق لتعزيز أمن المعلومات على المدى الطويل:

- الحوكمة سلطة وليست إنتاجاً: أثبتت الدراسة أن قوة الحوكمة الرقمية تكمن في قدرتها على فصل سلطة اتخاذ القرار عن عمليات الإنتاج التقني، مما يضمن وجود رقابة مستقلة ومساءلة واضحة تحمي المصالح الرقمية للمؤسسة.

- تكامل "ثالوث CIA" والحوكمة: لا يمكن تحقيق (السرية، السلامة، التوافر) كعناصر تقنية بحتة؛ بل إن الحوكمة هي التي توفر الإطار التنظيمي والسياسات التي تضمن استمرارية هذه العناصر وحمايتها من التهديدات المتطورة.

- أنسنة التكنولوجيا عبر الأخلاقيات: برز البعد الأخلاقي كركيزة أساسية؛ حيث إن حماية البيانات ليست مجرد امتثال قانوني، بل هي التزام أخلاقي باحترام خصوصية الفرد وكرامته، وهو ما يبني الثقة المستدامة بين المؤسسة وأصحاب المصلحة.

- التحدي البشري والتشريعي: كشفت الدراسة أن "الحلقة الأضعف" تظل متمثلة في ضعف الوعي الرقمي لدى العنصر البشري، وفجوة التشريعات التي غالباً ما تلهث خلف التطور المتسارع للهجمات السيبرانية.

- التحول من الدفاع التفاعلي إلى الاستباقي: دمج تقنيات الذكاء الاصطناعي والبلوكتشين في إطارات الحوكمة يسمح للمؤسسات بالانتقال من انتظار وقوع الحادث (Reaction) إلى التنبؤ بالمخاطر ومنعها (Proaction).

- توصيات ومقترحات:

بناء على ما تقدم، نضع مجموعة من المقترحات لتعزيز كفاءة الحوكمة الرقمية في حماية أمن المعلومات:

على المستوى التنظيمي:ضرورة تبني سياسات أمن معلومات (ISPs) مرنة وغير ثابتة، يتم تحديثها دوريا بناء على تقييم المخاطر (Risk-Based Approach) وليس فقط الامتثال لقوائم المراجعة التقليدية.

تفعيل نظام التحكم في الوصول القائم على الأدوار (RBAC) بشكل صارم لضمان حصر الصلاحيات في أضيق الحدود اللازمة للعمل.

على مستوى بناء القدرات:إطلاق برامج محو الأمية الرقمية والأمنية المكثفة للموظفين والمواطنين، مع التركيز على التصدي لهندسة الاجتماع (Social Engineering).

تحويل "الأمن السيبراني" من مهمة تقنية في قسم الحاسب الآلي إلى "هوية قيادية" تتبناها الإدارة العليا في المؤسسة.

على المستوى التقني والتشريعي:الاستثمار في أنظمة الرقابة الآلية والذكية التي تعتمد على التعلم الآلي لرصد الأنماط الشاذة في الوقت الفعلي.

حث المشرعين على تطوير أطر قانونية استباقية تتماشى مع المعايير الدولية مثلGDPR))، لسد الثغرات التنظيمية التي يستغلها المهاجمون.

على مستوى البحث العلمي:إجراء دراسات مستقبلية حول "حوكمة الذكاء الاصطناعي التوليدي" ومخاطره على خصوصية البيانات داخل المؤسسات الحكومية.

-الهوامش:

1-Aryanti, D. R. (2025). Cybersecurity Governance in Public Institutions: Managing Digital Risks and Resilience *Visioner*, *17*(03).

2-Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers Security*, *92*, 101776.

3-Buruiana, A. (2025). The Ethical Dimension of the Principle of Responsibility Regarding the Right to the Protection of Personal Data. *European Journal of Law Public Administration*, *12*(2), 121-137.

4-C.V, G. (2024). digital governance and cybersecurity: challenges in the age of egovernance. *journal of visual and performing arts*, *5*(1), 4328-4332.

5-Chen, W. (2024). *Digital Government Information Disclosure and Privacy Protection.* Paper presented at the 2024 4th International Conference on Public Relations and Social Sciences (ICPRSS 2024).

6-Dogou, M. (2025). A Future of Governance in the Digital Era. *Social Sience and Humanities Journal*, *09*(01), 6609.

7-Grigalashvili, V. (2023). Digital government and digital governance: grand concept. *International Journal of Scientific Management Research*, *6*(01), 01-25.

8-Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. J. J. o. B. R. (2023). Digital governance: A conceptual framework and research agenda. *162*, 113777.
9-Isabella, I., Agustian, E., Baharuddin, T., Ibrahim, A., & Regulation. (2025). Bridging e-government with digital literacy: A literature review. *Journal of Governance, 14*(1), 361-371.
10-Kehinde, S. (2025). Information governance frameworks for strengthening cybersecurity resilience in organizations. *Gulf Journal of Computer Sciences, 1*(4).
11-Korhonen, J. J., Hiekkanen, K., & Mykkänen, J. (2012). Information security governance. In *Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions* (pp. 53-66): IGI Global Scientific Publishing.
12-Magnusson, L., Iqbal, S., Elm, P., & Dalipi, F. (2025). Information security governance in the public sector: investigations, approaches, measures, and trends. *International Journal of Information Security, 24*(4), 177.
13-Malik, G. (2025). CYBERSECURITY GOVERNANCE AND RISK MANAGEMENT FOR DIGITAL TRANSFORMATION. *International Journal of Applied Mathematics, 38*(10s), 2532-2561.
14-Matei, A., & Bujac, R. (2016). Innovation and public reform. *Procedia Economics Finance, 39*, 761-768.
15-Muhammad, M. H. B., Abas, Z. B., Ahmad, A. S. B., & Sulaiman, M. (2024). AI-driven security: Redefining security information systems within digital governance. *nt. J. Res. Inf. Secur. Syst., 8090245*, 2923-2936.
16-Musa, N. (2018). *A conceptual framework of IT security governance and internal controls.* Paper presented at the 2018 Cyber Resilience Conference (CRC).
17-Naidu, K., & Chakravarthy, S. (2021). Legal Policies for Sustainable Security and Privacy in Big Data and Information sharing-A managerial perspective. *The Journal of Contemporary Issues in Business Government, 27*(2), 1556-1571.
18-Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T., & Kagaya, T. (2009). *Information security governance framework.* Paper presented at the Proceedings of the first ACM workshop on Information security governance.
19-Paselle, E., Indarto, K., & Rande, S. (2025). Digital Governance in Public Administration: Enhancing Transparency Through E-Government Platforms. *The Journal of Academic Science, 2*(2), 539-546.
20-Sax, M. (2018). Privacy from an ethical perspective. *he Handbook of Privacy Studies: An Interdisciplinary Introduction*, 143-172.
21-Setyarto, D. B., Alimuddin, A., Mulyaningsih, M., & Judijanto, L. (2025). The role of e-government in increasing transparency and accountability of public administration in the digital era. *Edelweiss Applied Science Technology Innovation Management Review, 9*(2), 1771-1783.
22-Shabbir, A., Anwar, A. S., Taslima, N., Sayem, M. A., Sikder, A. R., & Sidhu, G. S. (2024). Analyzing enterprise data protection and safety risks in cloud computing using ensemble learning. *International Journal on Recent Innovation Trends in Computing Communication, 12*(2), 499-507.
23-Sharma, A., Koohang, A., & Singh, S. P. J. J. o. G. I. M. (2025). Information Security Policy Compliance: a structured review using scientometric analysis and topic modeling. *33*(1), 1-32.
24-Wiltshire, D., & Alvanides, S. (2022). Ensuring the ethical use of big data: lessons from secure data access. *Heliyon, 8*(2).
25-Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education, 8*(2), 34-42.

26-Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *EEE access, 6*, 18209-18237.
27-Zul Afida Abdullah., R. H. (2026). Cybersecurity Leadership as Governance: A Constructivist Grounded Theory of Digital Risk Stewardship in Public Education. *INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE, 10*(2).