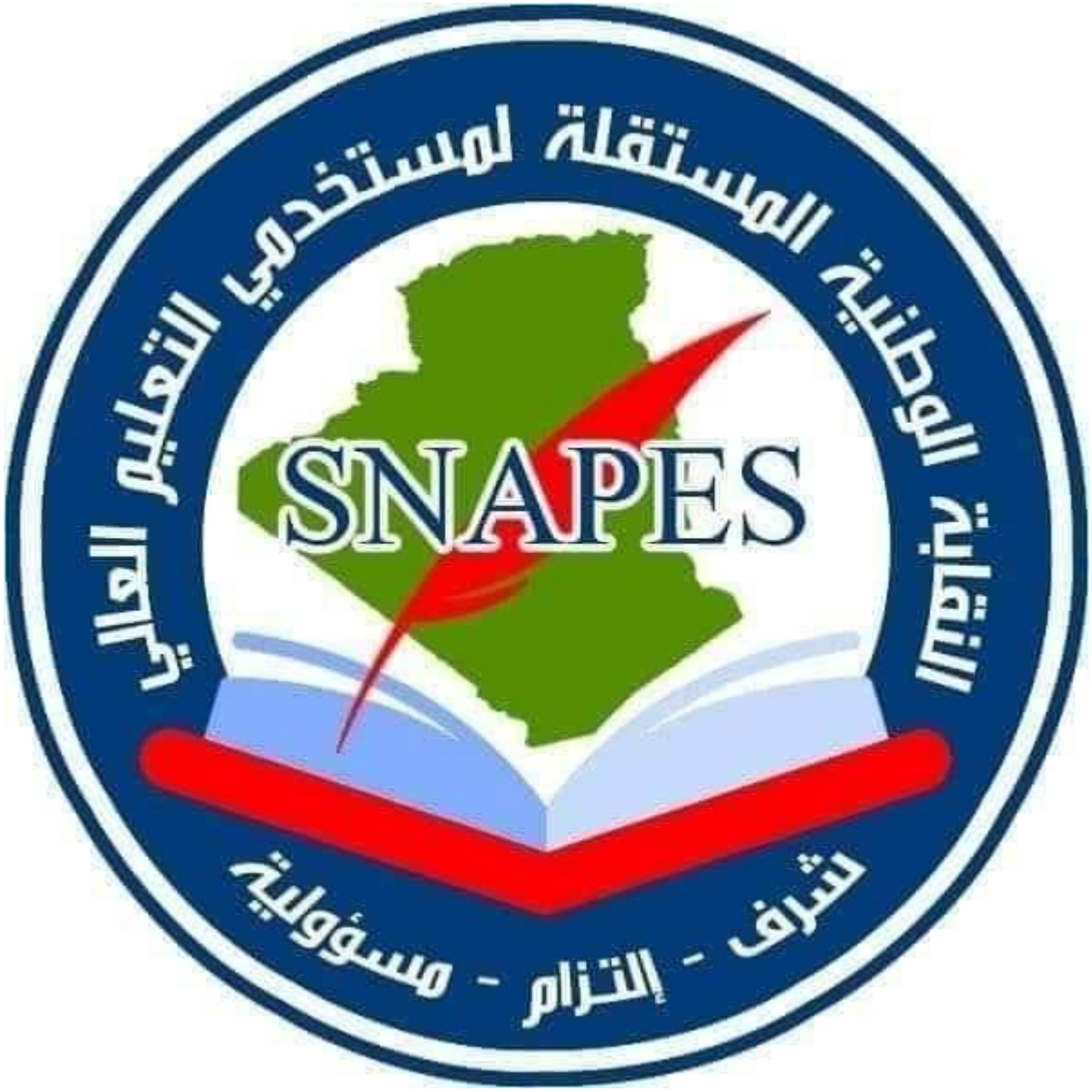

جامعة غرداية
UNIVERSITY OF GHARDAIA



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.

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

حوكمة :حول (حضوري وعن بعد) الملتقى الوطني الأول مؤسسات التعليم العالي

في ظل التحول الرقمي والتشريعات الحديثة.

مداخلة بعنوان:

الأمن المعلوماتي وأخلاقيات الحوكمة الرقمية
في مؤسسات التعليم العالي – تجارب رائدة

من إعداد الباحثين : من خلال المحور رقم: ..... .

من إعداد الباحثين : من خلال المحور رقم:04

أرحاب هلال وسام. أستاذة محاضرة أ، جامعة غرداية arhab.wissam@univ-ghardaia.edu.dz

الطبي عائشة، أستاذة محاضرة ب، جامعة غرداية .

الزهواني مروى، أستاذة محاضرة ب، جامعة غرداية .

ملخص

يتناول هذا البحث إشكالية الأمن المعلوماتي وأخلاقيات الحوكمة الرقمية في مؤسسات التعليم العالي، وذلك في ظل التحول الرقمي المتسارع الذي أعاد تشكيل البيئة المعلوماتية لهذه المؤسسات على المستويين التشغيلي والاستراتيجي. وتسعى الدراسة إلى تحليل المخاطر السيبرانية التي تتعرض لها الجامعات والكليات، واستعراض أُطر الحوكمة الرقمية الأخلاقية الكفيلة بتوفير الحماية اللازمة للبيانات، والمعلومات الأكاديمية والمالية والشخصية. اعتمدت الدراسة المنهج الوصفي التحليلي المقارن، مستعينةً بتجارب رائدة من جامعات

وتخلص الدراسة .دولية ومحلية أثبتت كفاءتها في تطبيق سياسات الأمن المعلوماتي وتعزيز الحوكمة الرقمية إلى أن غياب استراتيجية واضحة للحوكمة الرقمية يُفضي إلى ثغرات أمنية خطيرة تطال البيانات الأكاديمية كما تُؤكد أن تبني مبادئ الشفافية والمساءلة والمسؤولية الأخلاقية في إدارة .والمالية والشخصية على حدٍّ سواء وتوصي الدراسة بضرورة .المعلومات يُشكّل ركيزةً أساسية لاستدامة مؤسسات التعليم العالي في العصر الرقمي إنشاء وحدات متخصصة للحوكمة الرقمية داخل الجامعات، وسنّ تشريعات وطنية صارمة لحماية البيانات، كمرجعية إلزامية ISO/IEC 27001 واعتماد معايير دولية كـ.

الكلمات المفتاحية: الأمن المعلوماتي، الحوكمة الرقمية، التعليم العالي، الأخلاقيات الرقمية، حماية البيانات، الهجمات السيبرانية، ISO/IEC 27001.

Abstract

This research addresses the issue of information security and digital governance ethics in higher education institutions amid rapid digital transformation that has reshaped the informational landscape of universities at both operational and strategic levels. The study analyzes the cyber threats facing higher education institutions and examines ethical digital governance frameworks capable of ensuring adequate protection of academic, financial, and personal data. A comparative analytical-descriptive methodology was adopted, drawing on leading experiences from international and local universities that have demonstrated efficiency in implementing information security policies and strengthening digital governance. The study concludes that the absence of a clear digital governance strategy leads to serious security vulnerabilities affecting academic, financial, and personal data alike. It further emphasizes that embracing principles of transparency, accountability, and ethical responsibility in information management constitutes a fundamental pillar for the sustainability of higher education institutions in the digital age. The study recommends establishing specialized digital governance units within universities, enacting strict national data protection legislation, and adopting international standards such as ISO/IEC 27001 as a mandatory reference.

Keywords: Information Security, Digital Governance, Higher Education, Digital Ethics, Data Protection, Cyber Threats, ISO/IEC 27001.

مقدمة

يشهد العالم المعاصر ثورةً رقميةً غير مسبوقة أحدثت تحولات جذرية في بنية وقد باتت مؤسسات التعليم العالي تعتمد .المؤسسات التعليمية وأساليب إدارتها وتقديم خدماتها اعتماداً متزايداً على منظومات تقنية المعلومات والاتصالات في إدارة سجلاتها الأكاديمية والإدارية والمالية، مما جعلها أهدافاً جذابة للهجمات السيبرانية المتطورة (Anderson et al.,

وفي هذا السياق، يبرز الأمن المعلوماتي بوصفه أحد أعمدة الاستدامة المؤسسية، إذ لا .(2019 يقتصر دوره على الحماية التقنية بل يمتد ليشمل أبعاداً أخلاقية وحوكمية بالغة الأهمية.

وتُعدّ مؤسسات التعليم العالي بيئاتٍ معقدة من حيث تعدد أصحاب المصلحة وتنوع البيانات التي تتداولها، إذ تشمل بيانات الطلاب والأساتذة والبحوث العلمية والمعلومات المالية والاتفاقيات المؤسسية .وهذا التعقيد يستوجب نهجاً متكاملاً للحوكمة الرقمية يجمع بين الكفاءة التقنية والمسؤولية الأخلاقية والامتثال للأطر التشريعية والدولية (ENISA, 2021). وقد كشفت جائحة كوفيد-19 عن هشاشة كثير من أنظمة التعليم الرقمي وضعف آليات الحماية فيها، مما أفضى إلى تصاعد ملحوظ في معدلات الاختراقات الأمنية التي طالت مؤسسات أكاديمية بارزة حول العالم (Verizon, 2022).

وقد رصدت دراسات متعددة أن قطاع التعليم العالي أصبح الهدف الثالث الأكثر استقطاباً للهجمات السيبرانية على مستوى العالم بعد القطاع المالي والرعاية الصحية، وهو ما يستدعي من مؤسسات التعليم العالي إعادة النظر في منظوماتها الأمنية والحوكمية على نحو جذري وشامل (IBM Security, 2023). إن هذه الورقة البحثية تنطلق من إدراك عميق لحجم هذه التحديات، وتسعى إلى تقديم تحليل علمي رصين يستند إلى تجارب دولية رائدة ومعايير عالمية محكمة، بهدف استخلاص توصيات قابلة للتطبيق.

إشكالية البحث

تتمحور إشكالية البحث الرئيسية حول التساؤل الآتي:

كيف يمكن لمؤسسات التعليم العالي أن تُحقق توازناً فعّالاً بين متطلبات الأمن المعلوماتي ومبادئ الحوكمة الرقمية الأخلاقية في ظل التحديات السيبرانية المتصاعدة؟

وتتفرع عن هذه الإشكالية الرئيسية التساؤلات الفرعية التالية:

- ما هي أبرز المخاطر السيبرانية التي تتعرض لها مؤسسات التعليم العالي في العصر الرقمي؟
- ما أُطر الحوكمة الرقمية الأخلاقية الملائمة لبيئة التعليم العالي؟
- ما أبرز التجارب الدولية الرائدة في تطبيق سياسات الأمن المعلوماتي بالجامعات؟
- ما الآليات الكفيلة بتحقيق الامتثال للمعايير الدولية لأمن المعلومات في مؤسسات التعليم العالي؟
- كيف يُمكن الاستفادة من هذه التجارب الرائدة في تطوير المنظومة الأمنية للجامعات العربية؟

أهداف البحث

يرمي هذا البحث إلى تحقيق الأهداف الآتية:

- رصد وتحليل أبرز التهديدات والمخاطر السيبرانية الموجهة لمؤسسات التعليم العالي.
- استعراض أُطر الحوكمة الرقمية الأخلاقية وتقييم مدى ملاءمتها لبيئة التعليم العالي.
- دراسة تجارب دولية رائدة وتحليل نجاحاتها ودروسها المستخلصة.
- رصد التحديات الهيكلية والتنظيمية التي تُعيق تطبيق منظومة أمن معلوماتي فاعلة.
- تقديم توصيات عملية قابلة للتطبيق لمؤسسات التعليم العالي في الدول العربية والنامية.

منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي المقارن، من خلال مراجعة الأدبيات العلمية المتخصصة والتقارير الدولية ذات الصلة، إلى جانب تحليل دراسات الحالة للمؤسسات الرائدة في مجال الأمن المعلوماتي والحوكمة الرقمية. وتعتمد الدراسة على مصادر أولية وثانوية معتمدة، مع الاستناد إلى أحدث الإحصاءات والتقارير الصادرة عن منظمات دولية متخصصة كـ ENISA وGartner وISO. وقد اعتمد الباحث على مبدأ التثليث المنهجي (Methodological Triangulation) الجامع بين التحليل الكمي للإحصاءات المتاحة والتحليل النوعي للتجارب المؤسسية الرائدة.

المحور الأول: الأمن المعلوماتي في مؤسسات التعليم العالي – الإطار المفاهيمي والواقع الراهن

مفهوم الأمن المعلوماتي وأهميته في سياق التعليم العالي

يُعرَّف الأمن المعلوماتي (Information Security) بأنه مجموعة السياسات والإجراءات والتقنيات والممارسات الرامية إلى حماية المعلومات من الوصول غير المصرح به والتعديل والإفشاء والتدمير (ISO/IEC 27001:2022). ويرتكز على ثلاثية معروفة بـ CIA Triad، وهي: السرية (Confidentiality)، والتوافرية (Integrity)، والنزاهة (Availability). وقد طوّر الباحثون المصداقية (Authenticity)، في السنوات الأخيرة هذه الثلاثية لتشمل بُعدين إضافيين هما والمساءلة (Accountability)، مكوّنَيْن ما بات يُعرف بنموذج Parkerian Hexad (Whitman & Mattord, 2021).

وتكتسب هذه الأبعاد أهمية مضاعفة في سياق التعليم العالي نظراً لطبيعة البيانات المتداولة؛ فالسجلات الأكاديمية تحتوي على معلومات شخصية حساسة تستوجب السرية التامة، فيما

تتطلب نتائج البحوث العلمية والأطاريح الجامعية أعلى درجات النزاهة حمايةً لها من التزوير والانتحال، بينما تستدعي الموارد التعليمية الرقمية توافريةً مستدامة تكفل استمرارية العملية التعليمية. وقد رصد تقرير IBM X-Force Threat Intelligence Index لعام 2023 ارتفاعاً بنسبة 41% في الهجمات الموجهة لقطاع التعليم مقارنةً بعام 2020، مما يؤكد الأهمية الاستراتيجية لتعزيز منظومات الأمن المعلوماتي في هذا القطاع (IBM Security, 2023).

1.2 طبيعة المخاطر السيبرانية في مؤسسات التعليم العالي

تتميز البيئة الأمنية لمؤسسات التعليم العالي بخصائص تجعلها أكثر عرضة للتهديدات السيبرانية مقارنةً بكثير من القطاعات الأخرى. ومن أبرز هذه الخصائص: الطابع المفتوح للشبكات الجامعية الذي يُتيح الوصول لشرائح واسعة ومتنوعة من المستخدمين، وتعدد المستخدمين وتنوع مستويات وعيهم الأمني، وضخامة كميات البيانات المخزنة بما فيها بيانات أبحاث علمية ذات قيمة استراتيجية وتجارية عالية، فضلاً عن التمويل المحدود المخصص للأمن السيبراني قياساً بقطاعات أخرى كالمال والصناعة (Gartner, 2022).

وتتنوع التهديدات التي تواجهها هذه المؤسسات وتشمل: هجمات برامج الفدية (Ransomware) التي تُشلّ الأنظمة وتُهدد البيانات الحيوية وتتطلب فدية مالية ضخمة، وهجمات التصيد الاحتيالي (Phishing) التي تستهدف أعضاء هيئة التدريس والطلاب للحصول على بيانات اعتماد الدخول، والاختراقات الأمنية التي تستهدف قواعد بيانات البحوث العلمية ذات القيمة الاستراتيجية، إضافةً إلى التهديدات الداخلية الناجمة عن إساءة استخدام الصلاحيات من قِبَل موظفين أو طلاب (Ponemon Institute, 2022).

جدول (1): أبرز الإحصاءات المتعلقة بالتهديدات السيبرانية في قطاع التعليم العالي

المؤشر	المصدر / القيمة
متوسط تكلفة اختراق البيانات في التعليم العالي	3.86 مليون دولار (IBM Security, 2023)
نسبة الارتفاع في الهجمات على التعليم 2020-2023	41% (IBM X-Force, 2023)
ترتيب قطاع التعليم عالمياً في الاستهداف السيبراني	الثالث عالمياً (Verizon, 2022)
متوسط الإنفاق على أمن المعلومات في الجامعات	4-6% من ميزانية IT (EDUCAUSE, 2023)

الحد الأدنى الموصى به للإنفاق الأمني	10% من ميزانية IT (Gartner, 2022)

1.3 التشريعات والمعايير الدولية الناظمة للأمن المعلوماتي

أفرز التطور المتسارع للتهديدات السيبرانية ضرورةً ملحّة لاعتماد إطار تشريعي ومعياري دولي متين. من أبرز هذه الأطر معيار ISO/IEC 27001:2022 المتعلق بأنظمة إدارة أمن المعلومات (ISMS)، إذ يُوفر منهجية شاملة لإدارة المخاطر وضبط الضوابط الأمنية عبر دورة حياة Plan-Do-Check-Act. ويُعدّ هذا المعيار نقطة مرجعية دولية اعتمدتها مؤسسات أكاديمية كبرى كمعهد MIT وجامعة أكسفورد (ISO, 2022).

على الصعيد التشريعي الإقليمي والمحلي، تبرز اللائحة الأوروبية العامة لحماية البيانات (GDPR 2016/679) التي فرضت إطاراً صارماً لحماية البيانات الشخصية بما فيها بيانات الطلاب الأوروبيين، مع عقوبات مالية رادعة تصل إلى 4% من الإيرادات السنوية العالمية للمؤسسة. كما يبرز قانون FERPA الأمريكي الناظم لخصوصية السجلات التعليمية، وإطار NIST Cybersecurity Framework الذي اعتمدته كثير من الجامعات الأمريكية كمرجعية للأمن السيبراني (European Parliament, 2016; NIST, 2018).

أما على المستوى العربي، فقد أصدرت عدة دول أطراً تشريعية لحماية البيانات، من أبرزها: نظام حماية البيانات الشخصية السعودي (PDPL) لعام 2021، وقانون حماية البيانات الشخصية الإماراتي لعام 2021، فضلاً عن الاستراتيجية الوطنية للأمن السيبراني في المغرب. وتونس والأردن غير أن تطبيق هذه التشريعات على مؤسسات التعليم العالي لا يزال في طور التبلور والنضج.

المحور الثاني: أخلاقيات الحوكمة الرقمية في مؤسسات التعليم العالي

2.1 مفهوم الحوكمة الرقمية الأخلاقية وأبعادها

تُعرَّف الحوكمة الرقمية (Digital Governance) بأنها المنظومة المتكاملة من السياسات والإجراءات وآليات اتخاذ القرار المتعلقة بتوظيف الأصول الرقمية وإدارة البيانات ضمن المؤسسة (De Haes & Van Grembergen, 2015). وحين تضاف إليها البُعد الأخلاقي، تتحول إلى منظومة تكفل توازناً دقيقاً بين الكفاءة التشغيلية والمسؤولية الاجتماعية واحترام حقوق الأفراد.

أولاً، الشفافية: وتتمحور أخلاقيات الحوكمة الرقمية حول خمسة مبادئ جوهرية مترابطة (Transparency) وتعني وضوح القواعد الناظمة لجمع البيانات واستخدامها ومشاركتها مع جميع أصحاب المصلحة. ثانياً، المساءلة (Accountability) وتعني تحديد الجهات المسؤولة عن

وضمان حق (Privacy) ثالثاً، احترام الخصوصية .قرارات الحوكمة الرقمية وآليات محاسبتها وتعني (Digital Equity) رابعاً، الإنصاف والعدالة الرقمية .الأفراد في التحكم ببياناتهم الشخصية المتعلقة (Sustainability) خامساً، الاستدامة .ضمان المساواة في الوصول إلى الموارد الرقمية بالتداعيات البيئية والاجتماعية للبنية التحتية الرقمية (Janowski, 2015).

2.2 نماذج الحوكمة الرقمية في مؤسسات التعليم العالي

تتباين نماذج الحوكمة الرقمية المعتمدة في مؤسسات التعليم العالي عالمياً، ويمكن تصنيفها ضمن ثلاثة أنماط رئيسية :أولاً، النموذج المركزي الذي تتولى فيه وحدة مركزية متخصصة قيادة منظومة الحوكمة الرقمية وضبط معاييرها، وهو النموذج المعتمد في معظم الجامعات البريطانية العريقة .ثانياً، النموذج اللامركزي الذي يمنح الكليات والأقسام هامشاً أوسع من الاستقلالية في إدارة أصولها الرقمية، مما يُتيح مرونة أكبر لكن على حساب التجانس المعياري .ثالثاً، النموذج الهجين الذي يجمع بين مزايا النموذجين السابقين ويُعدّ الأكثر انتشاراً في الجامعات الأمريكية والأوروبية الكبرى (EDUCAUSE, 2023).

وقد برز في السنوات الأخيرة توجه متصاعد نحو تأسيس مكاتب متخصصة لمسؤول أمن المعلومات الرئيسي (CISO) وكبير مسؤولي البيانات (CDO) داخل الهياكل التنظيمية للجامعات. ووفقاً لتقرير EDUCAUSE (2023) فإن 73% من الجامعات الأمريكية الكبرى تضم حالياً منصب CISO مقارنةً بـ 45% فقط عام 2015، مما يعكس تحولاً نوعياً في نظرة هذه المؤسسات إلى قضايا الأمن والحوكمة الرقمية.

2.3 التقاطع بين الأمن المعلوماتي والأخلاقيات في السياق الأكاديمي

يُولِّد التقاطع بين الأمن المعلوماتي والأخلاقيات في السياق الأكاديمي توتراً ظاهرياً بين الأمن الذي يميل نحو التقييد والضبط، والحرية الأكاديمية التي تتطلب :قيمتين متنافستين أولها سياسات الوصول إلى :ويمكن رصد هذا التوتر في ثلاثة محاور .الانفتاح وتدفق المعرفة وثانيها إدارة حقوق الملكية .قواعد البيانات البحثية بين الانفتاح العلمي ومتطلبات السرية وثالثها ضوابط نشر نتائج .(Open Access) الفكرية الرقمية في ظل ثورة المصادر المفتوحة الأبحاث الحساسة ذات التداعيات الأمنية أو الأخلاقية (Floridi et al., 2018).

وجامعة ستانفورد أطراً أخلاقية متكاملة MIT وقد طوّرت مؤسسات رائدة كجامعة Privacy تضمن التوازن بين قيمة الانفتاح العلمي ومتطلبات الأمن الأكاديمي، مستندةً إلى مبدأ الذي يُرسّخ حماية الخصوصية كسمة مدمجة في تصميم الأنظمة لا كطبقة إضافية by Design لاحقة (MIT Office of the CIO, 2022). ويُجسّد هذا المبدأ تحولاً فكرياً جوهرياً في ثقافة الحوكمة الرقمية الأكاديمية من منطق التقييد إلى منطق التمكين الآمن.

2.4 إشكاليات وحلول :حوكمة البيانات البحثية

تُمثّل البيانات البحثية أثمن الأصول المعلوماتية لمؤسسات التعليم العالي، وهي في الوقت ذاته من أعقد ملفات الحوكمة الرقمية. فالبيانات البحثية تتضمن في الغالب معلومات حساسة عن المشاركين في الدراسات، ونتائج علمية ذات قيمة تجارية واستراتيجية، وبيانات ممولة من الحكومات أو القطاع الخاص وفق شروط استخدام مقيدة (Dencik et al., 2019).

وقد أجابت مجتمعات العلم المفتوح على هذه الإشكاليات بوضع مبادئ FAIR لإدارة البيانات البحثية (Findable, Accessible, Interoperable, Reusable)، التي تسعى إلى تحقيق أقصى قدر من إتاحة البيانات البحثية دون الإخلال بمتطلبات الأمن والخصوصية. غير أن تطبيق هذه المبادئ على أرض الواقع لا يزال يُثير جدلاً واسعاً بين مجتمعات البحث العلمي، لا سيما في التخصصات التي تتعامل مع بيانات الأفراد أو المعلومات الحساسة ذات الأبعاد الأمنية (Wilkinson et al., 2016).

2.5 دور القيادة الأكاديمية في تعزيز ثقافة الحوكمة الرقمية

لا تقتصر مسؤولية الحوكمة الرقمية الأخلاقية على الأقسام التقنية المتخصصة، بل تمتد لتشمل القيادة الأكاديمية العليا من رؤساء الجامعات وعمداء الكليات وأعضاء مجالس الأمناء. وقد أثبتت الدراسات أن المؤسسات التي تتمتع قياداتها بوعي رقمي عالٍ وتلتزم شخصياً بمبادئ الحوكمة الرقمية الأخلاقية تُحقق نتائج أمنية أفضل بكثير من تلك التي تترك هذا الملف حكراً على الفريق التقني (WEF, 2022).

وتكتسب هذه المسألة أهمية مضاعفة في ضوء الطبيعة متعددة الأبعاد للحوكمة الرقمية، التي تمسّ جوانب القانون والمالية والموارد البشرية والعلاقات العامة إلى جانب الجانب التقني. ولهذا تتجه كثير من الجامعات الرائدة نحو دمج برامج تطوير الكفاءات الرقمية للقيادات الأكاديمية ضمن خططها الاستراتيجية للتحول الرقمي، بما في ذلك دورات متخصصة في أخلاقيات البيانات والأمن السيبراني مُصمَّمة خصيصاً للمسؤولين الأكاديميين غير المتخصصين في التقنية (EDUCAUSE, 2023).

2.6 المسؤولية الاجتماعية للجامعات في الفضاء الرقمي

تحمل مؤسسات التعليم العالي مسؤولية اجتماعية مزدوجة في الفضاء الرقمي؛ فهي من جهة مؤسسات مُنتِجة للمعرفة الرقمية ومُشكِّلة لوعي الأجيال القادمة، ومن جهة أخرى مؤسسات مستخدِمة للتقنية الرقمية في أداء رسالتها التعليمية والبحثية. وهذا الدور المزدوج يُلقي عليها عبئاً أخلاقياً وتنموياً لا تتحمله مؤسسات أخرى بالدرجة ذاتها (Floridi et al., 2018).

ويتجلى هذا البُعد المسؤولي بوضوح في مسألة الفجوة الرقمية (Digital Divide)؛ إذ تقع على عاتق الجامعات مسؤولية ضمان تكافؤ فرص الوصول الرقمي بين طلابها بصرف النظر عن خلفياتهم الاجتماعية والاقتصادية. كما يمتد ليشمل حماية الطلاب من التحرش الإلكتروني والتضليل المعلوماتي وغيرها من مخاطر الفضاء الرقمي التي باتت تُسبّب أضراراً نفسية واجتماعية بالغة. وقد طوّرت جامعات رائدة كجامعة ميلبورن الأسترالية وجامعة تورنتو الكندية سياسات متكاملة لحماية الطلاب رقمياً تُجسّد هذا البُعد المسؤولي بشكل ملموس.

المحور الثالث: تجارب رائدة في تطبيق الأمن المعلوماتي والحوكمة الرقمية

3.1 تجربة معهد ماساتشوستس للتكنولوجيا (MIT) – الولايات المتحدة الأمريكية

يُمثّل معهد MIT نموذجاً مثالياً في دمج متطلبات الأمن المعلوماتي مع ثقافة الانفتاح التي تُركّز على ثلاثة محاور. فقد أطلق المعهد مبادرة "MIT Cybersecurity@CSAIL" الأكاديمي المتكاملة في مجال: الاستجابة للحوادث الأمنية، وتعليم الأمن السيبراني، وإجراء أبحاث متقدمة في الأمن الرقمي. واعتمد المعهد نموذج Zero Trust Architecture الذي يفترض أن أي كيان داخل الشبكة أو خارجها يمثل تهديداً محتملاً، مع تطبيق مبدأ الحد الأدنى من الصلاحيات (Least Privilege) لجميع المستخدمين (MIT Office of the CIO, 2022).

كما أسس MIT لجنة حوكمة البيانات (Data Governance Committee) التي تضم ممثلين من مختلف الأقسام الأكاديمية والإدارية، وتتبنى التزاماً صريحاً بمبادئ FAIR لإدارة البيانات البحثية. وقد أتاحت هذه المقاربة المتكاملة خفض معدل الحوادث الأمنية بنسبة 60% مع الحفاظ على مستوى رفيع من الانفتاح الأكاديمي، وأكثر من 3,500 مشروع بحثي نشط مفتوح المصدر خلال الفترة 2018-2022. ويُقدّم هذا النموذج دليلاً ملموساً على أن الأمن المعلوماتي القوي لا يُعارض الحرية الأكاديمية بل يصونها ويحميها (Wilkinson et al., 2016).

3.2 تجربة جامعة أكسفورد – المملكة المتحدة

طوّرت جامعة أكسفورد إطاراً متكاملاً للحوكمة الرقمية يستند إلى استراتيجية "Oxford Digital Transformation" التي تُوازن بين الابتكار الرقمي ومتطلبات الأمن والامتثال. اعتمدت الجامعة شهادة Cyber Essentials Plus البريطانية وحصلت على اعتماد ISO/IEC 27001 يضمن التحقق الدقيق (IAM) لأنظمتها الحيوية، مع تطبيق نظام متطور لإدارة الهوية والوصول من هويات المستخدمين عبر تقنية المصادقة متعددة العوامل (MFA) (University of Oxford, 2022).

وعلى صعيد الحوكمة الأخلاقية، أسست أكسفورد "Oxford Internet Institute" المتخصص في دراسة الأبعاد الاجتماعية والأخلاقية للتحول الرقمي، ووضعت لجنة أخلاقيات البيانات مبادئ توجيهية واضحة لجمع البيانات البحثية واستخدامها. كما أنشأت الجامعة فريقاً

يعمل بالتنسيق مع المركز الوطني البريطاني (CSIRT) متخصصاً للاستجابة للحوادث السيبرانية 72 مما أسهم في تقليص متوسط وقت الاستجابة للحوادث الأمنية من ،(NCSC) للأمن السيبراني 2019-2022 (Dencik et al., 2019) ساعات خلال الفترة 4 ساعة إلى أقل من.

3.3 تجربة الجامعة الأمريكية في الشارقة – الإمارات العربية المتحدة

من أبرز النماذج الإقليمية في مجال الأمن (AUS) تُعدّ الجامعة الأمريكية في الشارقة فقد طوّرت الجامعة سياسة .المعلوماتي على مستوى التعليم العالي في منطقة الشرق الأوسط (NCSA) متكاملة لأمن المعلومات تنسجم مع متطلبات الهيئة الوطنية للأمن الإلكتروني الإماراتية، وتستوفي معايير ISO/IEC 27001. واعتمدت الجامعة نظام SIEM (Security Information and Event Management) لمراقبة الشبكات في الوقت الفعلي، وأنشأت مركزاً (SOC) لعمليات الأمن السيبراني يعمل على مدار الساعة (AUS, 2023).

وعلى صعيد الحوكمة، أسست الجامعة لجنة خاصة لأخلاقيات البحث الرقمي، ووفّرت ويُلاحظ أن الجامعة .برامج تدريبية دورية لجميع منسوبيها في مجال الوعي الأمني الرقمي أفادت من السياق التشريعي الإماراتي الذي شهد في السنوات الأخيرة تطوراً ملحوظاً، لا سيما والاستراتيجية الوطنية للأمن 2021 بعد صدور قانون الجرائم الإلكترونية المحدَّث عام ويمثل هذا النموذج الإقليمي مثالاً يُحتذى به للمؤسسات العربية .2021-2023 السيبراني الساعية إلى مواءمة منظوماتها مع أفضل الممارسات العالمية.

3.4 نحو نظام تعليم عالٍ آمن رقمياً :التجربة الكورية الجنوبية

انتهجت كوريا الجنوبية مقاربة وطنية شاملة في تأمين منظومة التعليم العالي رقمياً، من التي تتولى "Korea Education & Research Information Service (KERIS)" خلال تأسيس وتُتيح هذه الهيئة خدمات .تنسيق جهود الأمن السيبراني لجميع مؤسسات التعليم العالي الكورية مشتركة للأمن السيبراني وتدريباً وطنياً موحداً وبنية تحتية آمنة للبحوث الأكاديمية، بما في ذلك منصة سحابية حكومية محمية تجمع بين السرعة والأمان (KERIS, 2022).

وقد أسهمت هذه المقاربة الوطنية المنسقة في تخفيض تكاليف الأمن السيبراني مع تحقيق مستوى أمني أعلى بفضل ،40%و 30% للجامعات الكورية بنسبة تتراوح بين كما تضمنت هذه المقاربة برنامجاً وطنياً .الاستفادة من وفورات الحجم والخبرات المشتركة 1,500 لتدريب المختصين في الأمن السيبراني في قطاع التعليم يُخرّج سنوياً أكثر من متخصص على مستوى الدراسات العليا (KERIS, 2022).

3.5 مقارنة التجارب الرائدة واستخلاص الدروس

يُمكن من خلال المقارنة بين التجارب السابقة استخلاص جملة من الدروس الجوهرية:
أولاً، لا توجد وصفة سحرية موحدة تناسب جميع السياقات؛ إذ يتباين النموذج الأنسب تبعاً للسياق القانوني والمؤسسي والثقافي لكل جامعة. ثانياً، الاستثمار في الموارد البشرية المتخصصة لا يقل أهمية عن الاستثمار في التقنيات الأمنية، بل قد يفوقه في الأثر. ثالثاً، التعاون بين الجامعات والحكومات وهيئات الأمن السيبراني الوطنية يُحقق نتائج تفوق ما يمكن لأي مؤسسة تحقيقه منفردةً.

جدول (2): مقارنة التجارب الرائدة في الأمن المعلوماتي والحوكمة الرقمية

المؤسسة	أبرز الإنجازات
MIT – الولايات المتحدة	تخفيض الحوادث 60%
جامعة أكسفورد – المملكة المتحدة	ISO 27001
جامعة الشارقة – الإمارات	SOC 24/7
KERIS – كوريا الجنوبية	تخفيض تكاليف 30-40%

المحور الرابع: التحديات والآفاق المستقبلية

4.1 أبرز التحديات الهيكلية والتنظيمية:

تواجه مؤسسات التعليم العالي جملةً من التحديات الهيكلية التي تُعيق تطبيق منظومة أمن معلوماتي فاعلة. وفي مقدمة هذه التحديات شُح الموارد المالية المخصصة للأمن السيبراني؛ إذ تُشير دراسة EDUCAUSE (2023) إلى أن متوسط الإنفاق على أمن المعلومات في الجامعات لا يتجاوز 4-6% من ميزانيات تقنية المعلومات، وهو أقل بكثير من الحد الأدنى الموصى به عالمياً البالغ 10%.

يُضاف إلى ذلك شُح الكوادر البشرية المتخصصة في الأمن السيبراني؛ إذ يُقدّر المنتدى الاقتصادي العالمي (WEF) العجز العالمي في متخصصي الأمن السيبراني بأكثر من 3.4 مليون وظيفة شاغرة عام 2022، مما يجعل استقطاب هذه الكفاءات أمراً عسيراً للجامعات التي لا تستطيع منافسة القطاع الخاص في الرواتب والمزايا. كما تُشكّل ثقافة الأمن الرقمي في بيئة التعليم العالي تحدياً بالغاً، إذ يميل أعضاء هيئة التدريس والطلاب إلى إعطاء الأولوية للانفتاح

المعرفي على حساب قيود الأمن الرقمي، مما يُولّد مقاومة ضمنية لتطبيق السياسات الأمنية (Gartner, 2022).

4.2 تحديات حوكمة الذكاء الاصطناعي في التعليم العالي

يُفرز التوغل المتزايد لتطبيقات الذكاء الاصطناعي في البيئة الأكاديمية تحديات حوكمية وأخلاقية جديدة لم تكن مؤسسات التعليم العالي مُهيَّأة للتعامل معها. فالاستخدام المتصاعد لأدوات الذكاء الاصطناعي التوليدي في التحقق من الهوية وتقييم أداء الطلاب وإدارة المنصات الإلكترونية يُثير تساؤلات جدية حول الخصوصية والتحيز الخوارزمي والمساءلة. وتُضاف إلى ذلك مخاوف جديدة تتعلق بتوظيف الطلاب لهذه الأدوات في الغش الأكاديمي أو انتحال الهوية الأكاديمية (Floridi et al., 2018).

وقد استجابت بعض المؤسسات الرائدة لهذه التحديات بتطوير سياسات خاصة لحوكمة الذكاء الاصطناعي؛ فأصدرت جامعة هارفارد وثيقة "Responsible Use of Generative AI" عام 2023 كما التي تحدد الضوابط الأخلاقية لاستخدام هذه التقنيات في السياق الأكاديمي. طوّرت جامعة كامبريدج إطاراً شاملاً لأخلاقيات الذكاء الاصطناعي يتضمن لجان مراجعة متخصصة لتقييم المخاطر الأخلاقية لمشاريع الذكاء الاصطناعي قبل انطلاقها (Harvard University, 2023).

4.3 التحديات الخاصة بالجامعات في الدول النامية والعربية

تواجه مؤسسات التعليم العالي في الدول النامية والعربية تحديات مضاعفة تتعلق بمحدودية الموارد البشرية والمالية والبنية التحتية الرقمية من جهة، وتصاعد التهديدات السيبرانية الموجهة لها من جهة أخرى. وقد كشف تقرير المنظمة العربية لتقنية المعلومات والاتصالات (AICTO) لعام 2022 أن أكثر من 60% من الجامعات العربية لا تمتلك سياسة مكتوبة للأمن السيبراني، فيما تفتقر 75% منها إلى مسؤول مخصص للأمن المعلوماتي.

ويُفاقم من حدة هذه التحديات غياب الإطار التشريعي المتكامل لحماية بيانات التعليم العالي في كثير من الدول العربية، وضعف التعاون بين الجامعات فيما يخص تبادل المعلومات عن التهديدات السيبرانية، فضلاً عن الاعتماد الكبير على الحلول التقنية الجاهزة دون مواءمتها مع الاحتياجات المحلية. غير أن مبادرات وطنية واعدة في بعض الدول العربية كالإمارات والمملكة العربية السعودية والمغرب تُبشّر ببداية تحول إيجابي نحو منظومة أكاديمية أكثر أمناً وحوكمةً.

4.4 الآفاق المستقبلية: نحو جامعة آمنة ومسؤولة رقمياً

أولاً: تتشكّل ملامح الجامعة الآمنة رقمياً في المستقبل حول عدة محاور استراتيجية،
التي تُدرج متطلبات الأمن منذ مراحل (Security by Design) اعتماد مقاربة الأمن المدمج
ثانياً، الاستفادة من تقنيات الذكاء الاصطناعي وتعلم الآلة في. التصميم الأولى لأي نظام رقمي
ثالثاً، تطوير نماذج تشاركية للحوكمة. الكشف المبكر عن التهديدات والتنبؤ بها قبل وقوعها
الرقمية

تُشرك جميع أصحاب المصلحة من طلاب وأساتذة وإداريين في صنع قرارات الحوكمة
(Verizon, 2022).
ويتوقع المحللون أن يُتيح ظهور الحوسبة الكمية في العقد القادم قدرات هجومية غير مسبوقة
وفي المقابل، تُهيئ هذه التقنية فرصاً غير. ستجعل كثيراً من أنظمة التشفير الحالية عرضةً للكسر
وقد بدأ المعهد الوطني الأمريكي للمعايير. مسبوقة لتعزيز الأمن عبر التشفير الكمي المنيع
(Post-Quantum) بالفعل في وضع معايير التشفير ما بعد الكمي (NIST) والتكنولوجيا
ويستوجب ذلك من مؤسسات. (NIST, 2022) استعداداً لهذا التحول الجذري (Cryptography
التعليم العالي البدء الآن في التخطيط الاستراتيجي للانتقال نحو هذه المعايير الجديدة.

المحور الخامس: نحو إطار مقترح للأمن المعلوماتي والحوكمة الرقمية في الجامعات العربية

5.1 تشخيص الواقع الراهن للجامعات العربية

يتسم الواقع الراهن للأمن المعلوماتي والحوكمة الرقمية في الجامعات العربية بالتفاوت
ففي حين تتقدم بعض الجامعات في الإمارات والمملكة. الحاد بين المؤسسات وبين الدول ذاتها
العربية السعودية والأردن بخطوات ملموسة نحو تبني معايير دولية، تظل معظم الجامعات
وقد رصد تقرير المنظمة العربية. العربية في مراحل أولى من النضج المؤسسي في هذا المجال
من الجامعات العربية لا تمتلك 60% أن أكثر من (AICTO, 2022) لتقنية المعلومات والاتصالات
منها إلى مسؤول مخصص للأمن السيبراني 75% سياسة مكتوبة للأمن المعلوماتي، فيما تفتقر،
وهي أرقام تُشكّل إنذاراً مبكراً لصانعي السياسات والقيادات الأكاديمية.

ومن أبرز التحديات الخاصة بالسياق العربي: الاعتماد الكبير على الحلول التقنية الأجنبية
الجاهزة دون مواءمتها مع الاحتياجات المحلية واللغوية، وضعف الوعي بحقوق الخصوصية
الرقمية في الثقافة المؤسسية السائدة، وغياب ثقافة الإبلاغ عن الحوادث الأمنية خشية الإضرار
بسمعة المؤسسة، فضلاً عن محدودية التعاون بين الجامعات وهيئات الأمن السيبراني الوطنية
في بعض الدول.

5.2 مبادرات إقليمية واعدة

تتزامن هذه التحديات مع ظهور مبادرات إقليمية واعدة تُبشّر بتحول نوعي في المشهد
ومن أبرزها: في السيبراني للأمن السعودي الوطني البرنامج. الأمني لقطاع التعليم العالي العربي

بهدف رفع 2022 الذي أطلقته المملكة عام ،(NCA) التعليم التابع للهيئة الوطنية للأمن السيبراني مستوى النضج السيبراني في مؤسسات التعليم العالي وفق إطار .CSCC كذلك برز البرنامج الإماراتي لتصنيف المخاطر السيبرانية الأكاديمية الصادر عن الهيئة الوطنية للأمن الإلكتروني وهو أول برنامج عربي متخصص في تصنيف المخاطر للقطاع الأكاديمي ،2021 عام (NCSA) تحديداً.

وعلى الصعيد الإقليمي، أطلق مركز الأمن السيبراني التابع لجامعة الدول العربية عام ،منصة عربية مشتركة لتبادل المعلومات عن التهديدات السيبرانية بين الجامعات الأعضاء 2023 وهي خطوة رائدة نحو بناء منظومة تعاون أكاديمي عربي في مجال الأمن السيبراني على غرار النماذج الدولية الناجحة .تُشير التقديرات الأولية إلى أن هذه المبادرات أسهمت في رفع مؤشر النضج السيبراني لدى المؤسسات المشاركة بنسبة تتراوح بين 20% و35% فقط خلال عامين.

5.3 إطار مقترح متكامل للجامعات العربية

انطلاقاً من التحليل السابق للواقع والتجارب الرائدة، يقترح الباحث إطاراً متكاملاً يُلائم خصوصية السياق العربي ويُمكن تطبيقه على مراحل وفق المستوى التنظيمي والموارد المتاحة لكل مؤسسة .يقوم هذا الإطار على ثلاثة مستويات متدرجة :المستوى الأساسي، والمستوى المتوسط، والمستوى المتقدم؛ بما يتيح لكل مؤسسة تحديد موقعها الحالي والمسار الملائم للتطور.

يتضمن المستوى الأساسي: وضع سياسة أمن معلوماتي مكتوبة ومُعتمدة، وتعيين مسؤول للأمن السيبراني ولو بدوام جزئي، وتدريب الموظفين على أسس الوعي الأمني، وتطبيق الحد الأدنى من ضوابط ISO/IEC 27001. ويرتقي المستوى المتوسط ليشمل: إنشاء لجنة توجيهية للأمن السيبراني، وتطوير خطة استجابة للحوادث، وتطبيق حوكمة رقمية، واعتماد نظام إدارة الهوية والوصول (IAM). أما المستوى المتقدم فيستوجب: الحصول على اعتماد ISO/IEC 27001 الكامل، وإنشاء مركز عمليات أمن (SOC)، وتطبيق نموذج Zero Trust Architecture، وقيادة مبادرات التعاون الإقليمي.

5.4 مؤشرات قياس النضج الأمني والحوكمي في الجامعات

لا يكتمل أي إطار للأمن المعلوماتي والحوكمة الرقمية دون منظومة واضحة لقياس مستوى النضج وتتبع التحسين .ويقترح الباحث مجموعة من مؤشرات الأداء الرئيسية (KPIs) المُصمَّمة خصيصاً لقطاع التعليم العالي، تتوزع على محاور: الوقاية (نسبة تغطية منح الصلاحيات، ونسبة الأنظمة المُحدَّثة)، والاستجابة (متوسط وقت الاستجابة للحوادث، ومعدل الاستعادة بعد الكوارث)، والتوعية (نسبة منسوبي الجامعة الذين اجتازوا برنامج التوعية الأمنية)

ومتطلبات التشريعات ISO/IEC 27001 نسبة المعايير الدولية المُطبَّقة من) والامتثال ،(السنوي الوطنية).

ويُوصي الباحث بربط هذه المؤشرات بمنظومة التقييم الجامعي والاعتماد الأكاديمي، بحيث تُصبح متطلبات الأمن المعلوماتي والحوكمة الرقمية شرطاً ضمنياً من شروط الحصول على الاعتماد الأكاديمي وتجديده، على غرار ما بدأت تتجه إليه هيئات الاعتماد الأكاديمي في أوروبا وأمريكا الشمالية.

جدول (3): مستويات النضج الأمني المقترحة للجامعات العربية

المستوى	المتطلبات الأساسية
الأساسي	سياسة أمن مكتوبة
المتوسط	لجنة حوكمة
المتقدم	اعتماد ISO 27001

الخاتمة والتوصيات

أولاً: الخاتمة

خلصت هذه الدراسة إلى أن الأمن المعلوماتي وأخلاقيات الحوكمة الرقمية يُمثّلان ثنائياً متلازماً لا يمكن الفصل بينهما في سياق مؤسسات التعليم العالي. فالأمن بلا إطار أخلاقي يتحول إلى قيدٍ يُعيق الحرية الأكاديمية، والأخلاقيات بلا منظومة أمنية صلبة تبقى مجرد شعارات فارغة من أي محتوى عملي. وقد أثبتت التجارب الرائدة التي استعرضناها أن المؤسسات الأكاديمية القادرة على تحقيق هذا التوازن الدقيق هي من تنجح في بناء منظومة رقمية مستدامة وموثوقة وذات قدرة تنافسية متصاعدة.

وتؤكد الدراسة كذلك أن التحول الرقمي في التعليم العالي ليس ترفاً تكنولوجياً بل ضرورة استراتيجية، غير أن نجاح هذا التحول يتوقف توقفاً جوهرياً على توافر منظومة أمنية وحوكمية فاعلة. ومن أبرز ما أسفرت عنه الدراسة من نتائج: أن الدول التي اعتمدت مقاربة وطنية شاملة كنموذج KERIS الكوري حققت نتائج أفضل بكثير من تلك التي تركت المؤسسات

كما أن الاستثمار في الكوادر البشرية المتخصصة يُحقق .الأكاديمية تعمل منفردةً في هذا المجال عائداً على الاستثمار الأمني أعلى من الاستثمار في الأنظمة التقنية منفردةً.

التوصيات :ثانياً

بناءً على نتائج الدراسة وتحليل التجارب الرائدة، يوصي الباحث بما يلي:

1. إنشاء وحدات متخصصة للحوكمة الرقمية ضمن الهياكل التنظيمية لمؤسسات التعليم العالي، برئاسة مسؤول أمن معلومات رئيسي (CISO) ويرفع تقاريره مباشرةً إلى مجالس الأمناء، مع ضمان استقلاليته عن وحدة تقنية المعلومات.

2. اعتماد معيار ISO/IEC 27001:2022 كمرجعية إلزامية لجميع مؤسسات التعليم العالي، مع توفير دعم حكومي لتغطية تكاليف الحصول على هذا الاعتماد لا سيما للمؤسسات ذات الإمكانات المحدودة.

3. سنّ تشريعات وطنية متخصصة لحماية بيانات الطلاب والباحثين، مستلهِمةً من التجارب الأوروبية (GDPR) مع مراعاة الخصوصية الثقافية والتشريعية لكل دولة، مع التنسيق الإقليمي العربي لاعتماد إطار موحد.

4. إنشاء مراكز وطنية للتميز في الأمن السيبراني للتعليم العالي على غرار النموذج الكوري (KERIS)، تُوفر خدمات مشتركة وتدريباً موحداً وبنية تحتية سحابية آمنة مشتركة بين الجامعات.

5. دمج مقررات الأمن المعلوماتي والأخلاقيات الرقمية في المناهج الأكاديمية لجميع التخصصات، مع إلزامية برامج التوعية الأمنية السنوية لجميع منسوبي الجامعات بمختلف فئاتهم ومستوياتهم.

6. تطوير أطر أخلاقية واضحة لحوكمة الذكاء الاصطناعي في البيئة الأكاديمية، بما يضمن الاستخدام المسؤول لهذه التقنيات مع صون حقوق الطلاب والباحثين وضمان النزاهة الأكاديمية.

قائمة المراجع والمصادر

المراجع العربية :أولاً

.دار المريخ للنشر .(2 .ط) الفن والعلم :أمن الحاسوب .(2019) .وبارتولي، م ،.أندرسون، ر
تقرير الأمن السيبراني في التعليم العالي .(2022) .المنظمة العربية لتقنية المعلومات والاتصالات العربي. .جامعة الدول العربية

المراجع الأجنبية :ثانياً

- AUS – American University of Sharjah. (2023). Information security policy framework. https://www.aus.edu/offices/it/information-security
- De Haes, S., & Van Grembergen, W. (2015). Enterprise governance of information technology: Achieving alignment and value. Springer. https://doi.org/10.1007/978-3-319-14547-1
- Dencik, L., Hintz, A., Redden, J., & Treré, E. (2019). Exploring data justice: Conceptions, applications and directions. Information, Communication & Society, 22(7), 873–881. https://doi.org/10.1080/1369118X.2019.1606268
- EDUCAUSE. (2023). 2023 EDUCAUSE horizon report: Information security edition. https://doi.org/10.1145/educause2023-sec
- ENISA – European Union Agency for Cybersecurity. (2021). Cybersecurity in higher education. ENISA. https://doi.org/10.2824/164187
- European Parliament. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union. https://doi.org/10.3000/1977-091X.L_2016.119.eng
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
- Gartner. (2022). Top trends in cybersecurity 2022. Gartner Research. https://www.gartner.com/en/cybersecurity/trends
- Harvard University. (2023). Responsible use of generative AI at Harvard. Harvard University Information Technology. https://huit.harvard.edu/ai/guidelines
- IBM Security. (2023). IBM X-Force threat intelligence index 2023. IBM Corporation. https://www.ibm.com/reports/threat-intelligence
- ISO/IEC. (2022). ISO/IEC 27001:2022 – Information security management systems – Requirements. International Organization for Standardization. https://doi.org/10.3403/30280203
- Janowski, T. (2015). Digital government evolution: From transformation to contextualization. Government Information Quarterly, 32(3), 221–236. https://doi.org/10.1016/j.giq.2015.07.001

- KERIS – Korea Education and Research Information Service. (2022). Cybersecurity in Korean higher education: Annual report 2022. KERIS. https://www.keris.or.kr
- MIT Office of the CIO. (2022). Information security program annual report 2022. Massachusetts
- Institute of Technology. https://ist.mit.edu/security/annualreport
- NIST. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). National
- Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018
- NIST. (2022). Post-quantum cryptography standardization. National Institute of Standards and Technology. https://csrc.nist.gov/projects/post-quantum-cryptography
- Ponemon Institute. (2022). 2022 cost of insider threats global report. Proofpoint & Ponemon Institute. https://www.proofpoint.com/us/resources/analyst-reports/cost-of-insider-threats
- University of Oxford. (2022). Oxford digital transformation strategy 2022–2027. University of
- Oxford. https://www.ox.ac.uk/sites/files/oxford/digital-transformation-strategy.pdf
- Verizon. (2022). 2022 data breach investigations report. Verizon Business.
- https://doi.org/10.12871/978888798524-3
- Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (6th ed.). Cengage
- Learning. https://doi.org/10.1007/978-3-658-25765-1
- Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., ... & Mons, B. (2016). The FAIR guiding principles for scientific data management and stewardship. Scientific Data, 3, 160018. https://doi.org/10.1038/sdata.2016.18
- World Economic Forum. (2022). Global cybersecurity outlook 2022. World Economic Forum.

https://www.weforum.org/reports/global-cybersecurity-outlook-2022

1