

الأمن السيبراني وحماية البيانات في المكتبات الحديثة

Cybersecurity and Data Protection in Modern Libraries

د. قواسمية عبد الغني

جامعة الشيخ العربي التبسي تبسة (الجزائر)

abdelghani.gouasmia@univ-tebessa.dz

د. بزاوية زهرة*

جامعة وهران 1- أحمد بن بلة (الجزائر)

bezzaouyazohra303@gmail.com

المخلص:

معلومات المقال

يتناول هذا المقال موضوع الأمن السيبراني وحماية البيانات في المكتبات الحديثة في ظل التحول الرقمي، حيث أصبحت هذه المؤسسات أكثر عرضة للتهديدات الإلكترونية، وتهدف إلى تحليل المفاهيم الأساسية، واستعراض أبرز المخاطر مثل الهجمات السيبرانية وتسريب البيانات، إضافة إلى مناقشة آليات الحماية كالتشفير وأنظمة الأمن وإدارة الوصول. وخلص المقال إلى أن تحقيق أمن معلوماتي فعال في المكتبات يتطلب تكاملاً بين الحلول التقنية والتنظيمية، مع ضرورة تعزيز الوعي الأمني وتحديث الأنظمة بشكل مستمر لضمان حماية البيانات واستمرارية الخدمات.

تاريخ الإرسال: 2026/05/16
تاريخ القبول: 2026/06/13
تاريخ النشر: 2026/06/30

الكلمات المفتاحية:

- ✓ الأمن السيبراني
- ✓ حماية البيانات
- ✓ التحول الرقمي
- ✓ أمن المعلومات
- ✓ المكتبات الحديثة.

Abstract :

Article info

This article addresses cybersecurity and data protection in modern libraries within the context of digital transformation, a shift that has rendered these institutions increasingly susceptible to cyber threats. It seeks to examine the foundational concepts of cybersecurity, identify key risks—such as cyberattacks and data breaches—and discuss core protection mechanisms, including encryption, security systems, and access control management.

The article concludes that achieving effective information security in libraries requires a coordinated integration of technical and organizational measures. It further emphasizes the need to strengthen security awareness and to continuously update systems in order to ensure data protection and the continuity of library services

Received :16/05/2026
Accepted :13/06/2026
date of publication: 30/06/2026

Keywords:

- ✓ Cybersecurity
- ✓ Data Protection
- ✓ Digital Transformation
- ✓ Information Security
- ✓ Modern Libraries

1. مقدمة:

شهد العالم خلال العقود الأخيرة تحولات عميقة ومتسارعة بفعل الثورة الرقمية التي أعادت تشكيل مختلف القطاعات، وعلى رأسها قطاع المعلومات والمعرفة. فقد أدى التطور المتلاحق في تكنولوجيات المعلومات والاتصال إلى بروز بيئة رقمية جديدة تتسم بالتدفق الهائل للبيانات، وسرعة تداول المعلومات، واتساع نطاق الوصول إليها. وفي هذا السياق، لم تعد المؤسسات التقليدية بمنأى عن هذه التحولات، بل أصبحت مطالبة بإعادة تشكيل أدوارها ووظائفها بما يتلاءم مع متطلبات العصر الرقمي.

وثُعدّ المكتبات من أبرز المؤسسات التي شهدت هذا التحول، حيث انتقلت من كونها فضاءات تقليدية تُعنى بحفظ الكتب الورقية وتنظيمها، إلى نظم معلومات متكاملة تعتمد على البنى التحتية الرقمية والتطبيقات الذكية في إدارة المعرفة وإتاحتها. فلم يعد دور المكتبة مقتصرًا على الإعارة والخدمات المرجعية التقليدية، بل امتد ليشمل تقديم خدمات رقمية متقدمة مثل الفهارس الإلكترونية (OPAC)، والمستودعات المؤسسية، وخدمات الإعارة الرقمية، إضافة إلى دعم البحث العلمي عبر قواعد البيانات الإلكترونية.

✓ إشكالية الدراسة

لقد عرف التحول الرقمي بمزاياه العديدة، لكن بالمقابل صاحبه بروز تحديات جديدة، لعل أبرزها ما يتعلق بالأمن السيبراني (Cybersecurity) وحماية البيانات (Data Protection) إذ أصبحت المكتبات، باعتبارها مستودعات ضخمة للبيانات والمعلومات، هدفًا محتملاً للهجمات السيبرانية بمختلف أشكالها، مثل الاختراقات الأمنية، والبرمجيات الخبيثة، وهجمات حجب الخدمة (DDoS)، وتسريب البيانات الحساسة للمستخدمين، كما أن تزايد الاعتماد على الأنظمة الرقمية والشبكات المفتوحة يضاعف من حجم المخاطر المرتبطة بسلامة البيانات وسرية المعلومات.

ومن هنا تبرز أهمية هذا الموضوع، خاصة في ظل التوجه العالمي نحو إتاحة المعلومات (Open Access) وتعزيز الشفافية الرقمية، وهو ما يطرح تحديًا حقيقيًا يتمثل في كيفية تحقيق التوازن بين إتاحة المعرفة من جهة، وضمان أمن المعلومات وحماية خصوصية المستخدمين من جهة أخرى.

انطلاقًا مما سبق، تتمحور إشكالية هذه الدراسة حول التساؤل الرئيسي الآتي:

كيف يمكن للمكتبات الحديثة تحقيق التوازن بين إتاحة المعلومات بشكل مفتوح وفعال، وبين ضمان حماية البيانات من التهديدات السيبرانية المتزايدة؟

ويتفرع عن هذا التساؤل مجموعة من الأسئلة الفرعية:

• ما المقصود بالأمن السيبراني في سياق المكتبات الحديثة؟

• ما أبرز التهديدات والمخاطر الرقمية التي تواجه المكتبات؟

• ما الآليات والتقنيات المعتمدة في حماية البيانات داخل هذه المؤسسات؟

• ما دور السياسات والتشريعات في تعزيز أمن المعلومات في البيئة المكتبية؟

✓ **أهداف الدراسة:** تسعى هذه الدراسة إلى تحقيق جملة من الأهداف العلمية والعملية، تتمثل فيما يلي:

يلي:

- تحليل مفهوم الأمن السيبراني وتحديد أبعاده في سياق المكتبات الحديثة
 - إبراز طبيعة التهديدات السيبرانية والمخاطر الرقمية التي تواجه نظم المعلومات المكتبية
 - استعراض أهم الآليات التقنية والتنظيمية المعتمدة في حماية البيانات
 - مناقشة دور التشريعات والسياسات في تأمين البيئة الرقمية للمكتبات
 - تقديم توصيات عملية من شأنها تعزيز أمن المعلومات وضمان استمرارية الخدمات المكتبية
- ✓ **منهجية الدراسة:** اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، باعتباره الأنسب لدراسة الظواهر المعاصرة وتحليل أبعادها المختلفة، حيث تم من خلاله:
- وصف واقع الأمن السيبراني في المكتبات الحديثة
 - تحليل المفاهيم الأساسية المرتبطة بحماية البيانات
 - دراسة التهديدات الرقمية وآليات مواجهتها
- كما تم الاعتماد على تحليل الأدبيات العلمية والدراسات السابقة ذات الصلة، بالإضافة إلى التقارير الصادرة عن الهيئات الدولية المتخصصة في أمن المعلومات، وذلك بهدف بناء إطار نظري متكامل يدعم موضوع الدراسة.

2. الإطار المفاهيمي

1.2 تعريف الأمن السيبراني:

يُعرّف الأمن السيبراني بأنه مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من الهجمات الرقمية أو الوصول غير المصرح به، ويتجاوز هذا المفهوم الجانب التقني ليشمل أيضاً البعد التنظيمي والبشري، حيث يعتمد بشكل كبير على وعي المستخدمين وسلوكهم (Von Solms & Van Niekerk, 2013).

كما تُعرّف المنظمة الدولية للمعايير (ISO) ضمن إطار المواصفة ISO/IEC 27032 بأنه: "حماية الفضاء السيبراني من التهديدات التي تستهدف ترابط الأنظمة والشبكات والبنى التحتية الرقمية" (ISO, 2012).

ويشير المعهد الوطني للمعايير والتكنولوجيا (NIST) إلى أن الأمن السيبراني يتمثل في: "القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات السيبرانية." (NIST, 2018) من جهة أخرى، يعرّف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني بأنه: "مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات وإدارة المخاطر والتدريب وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية ومستخدميها." (ITU, 2018) كما يرى (Craig, Diakun-Thibault, & Purse, 2014) أن الأمن السيبراني هو: "مجال متعدد التخصصات يركز على حماية المعلومات والأنظمة من التهديدات، مع ضمان توافرها وسريتها وسلامتها في سياق المكتبات، يشير الأمن السيبراني إلى حماية أنظمة إدارة المكتبات، وقواعد البيانات، وحسابات المستخدمين، والمحتوى الرقمي من أي تهديدات قد تؤدي إلى تعطيل الخدمات أو تسريب المعلومات، خاصة في ظل الاعتماد المتزايد على الأنظمة الرقمية والشبكات المفتوحة."

2.2 مفهوم حماية البيانات

تُعرّف حماية البيانات بأنها عملية ضمان سرية وسلامة وتوافر المعلومات، وتشمل حماية البيانات الشخصية للمستفيدين، مثل سجلات الإعارة والبحث، وكذلك البيانات المؤسسية الحساسة. ويُعد هذا المفهوم جزءاً أساسياً من الأمن السيبراني، خاصة في ظل تزايد الاعتماد على الأنظمة السحابية. (Kshetri, 2021) وتُعرّف اللائحة العامة لحماية البيانات الأوروبية (GDPR) حماية البيانات بأنها: "مجموعة من المبادئ والقواعد التي تهدف إلى حماية البيانات الشخصية وضمان معالجتها بشكل قانوني وعادل وشفاف. (European Union, 2016)" كما يشير (Peltier, 2016) إلى أن حماية البيانات هي: "مجموعة من السياسات والإجراءات والتقنيات التي تُطبّق لحماية البيانات من فقدان أو التلف أو الوصول غير المصرح به، عبر مختلف مراحل دورة حياتها." ويعرّف البرنامج العربي لأمن المعلومات حماية البيانات بأنها: "جملة التدابير التقنية والتنظيمية التي تُتخذ لضمان حماية البيانات من الاختراق أو سوء الاستخدام، مع الحفاظ على خصوصية الأفراد وسرية المعلومات" (المنظمة العربية لتكنولوجيات الاتصال والمعلومات، 2019)

كما يُعرّف (Alshammari & Simpson, 2017) حماية البيانات على أنها: "إطار شامل يهدف إلى حماية البيانات الحساسة من التهديدات الداخلية والخارجية، مع ضمان الامتثال للتشريعات والسياسات المنظمة للخصوصية." في سياق المكتبات، تكتسب حماية البيانات أهمية خاصة نظراً لطبيعة المعلومات التي تتعامل معها هذه المؤسسات، والتي تشمل بيانات المستخدمين وسجلاتهم البحثية، مما يستدعي اعتماد سياسات واضحة وآليات فعالة لضمان حماية الخصوصية وتعزيز الثقة في الخدمات الرقمية المقدمة.

2.3 المكتبات الحديثة والتحول الرقمي

تُعرّف المكتبات الحديثة بأنها مؤسسات معلوماتية متطورة تعتمد على تكنولوجيات المعلومات والاتصال في تنظيم المعرفة وإدارتها وإتاحتها، حيث لم تعد مجرد فضاءات مادية لحفظ الأوعية الورقية، بل تحولت إلى بيئات رقمية ديناميكية تدعم الوصول المفتوح للمعلومات وتسهّل التفاعل مع مصادرها. ويشير (Borgman, 2000) إلى أن المكتبات الرقمية تمثل "امتداداً للنظم التقليدية، لكنها تعتمد على بنى رقمية تتيح الوصول إلى المعلومات عبر الشبكات". كما يرى (Arms, 2000) أن المكتبة الحديثة هي "نظام متكامل يوفر موارد رقمية وخدمات معلوماتية عبر الإنترنت، مع ضمان تنظيمها وإتاحتها بكفاءة." كما تُعرّف المكتبات الحديثة بأنها:

"مؤسسات تعتمد على التقنيات الرقمية في تقديم خدمات معلوماتية متطورة، بما يحقق سرعة الوصول ودقة الاسترجاع وتوسيع قاعدة المستفيدين" (قاسم، 2018)

أ- مسار التحول الرقمي في المكتبات

لم يكن التحول الرقمي في المكتبات عملية فجائية، بل مرّ بعدة مراحل متدرجة، يمكن تلخيصها فيما يلي:

٧ مرحلة الأتمتة (Automation)

- إدخال الحواسيب لإدارة العمليات الداخلية
- استخدام أنظمة الفهرسة الإلكترونية بدل البطاقات الورقية
- ظهور أنظمة مثل *Integrated Library Systems (ILS)*

٨ مرحلة الرقمنة (Digitization)

- تحويل الكتب والوثائق الورقية إلى صيغ رقمية
- إنشاء المكتبات الرقمية (*Digital Libraries*)
- حفظ التراث الوثائقي إلكترونياً

٩ مرحلة الشبكات والاتصال (Networking)

- ربط المكتبات عبر الإنترنت
- ظهور الفهارس الموحدة (*Union Catalogs*)
- إتاحة البحث عن بُعد

١٠ مرحلة الخدمات الإلكترونية (E-Services)

- الفهارس الإلكترونية (*OPAC*)
- الإعارة الرقمية
- قواعد البيانات الإلكترونية

١١ مرحلة التحول الرقمي الشامل (Digital Transformation)

- الاعتماد على الحوسبة السحابية (*Cloud Computing*)
- استخدام الذكاء الاصطناعي في البحث والتوصية
- تحليل سلوك المستخدمين
- تقديم خدمات مخصصة (*Personalized Services*)

ب- مظاهر التحول الرقمي في المكتبات

- وقد أدى هذا التحول إلى مجموعة من التغيرات الجوهرية، من أبرزها:
- رقمنة المجموعات: تحويل الأوعية التقليدية إلى موارد رقمية قابلة للوصول عبر الإنترنت
- توفير الوصول عن بُعد: تمكين المستخدمين من استخدام خدمات المكتبة دون الحضور الفيزيائي
- استخدام أنظمة إدارة المكتبات المتكاملة: (*ILS*) لإدارة الفهرسة، الإعارة، والمقتنيات
- الاعتماد على الحوسبة السحابية: لتخزين البيانات وإدارة الخدمات بكفاءة ومرونة
- التكامل مع قواعد البيانات العالمية: لدعم البحث العلمي

ج- تحديات التحول الرقمي

- على الرغم من المزايا الكبيرة للتحول الرقمي، إلا أنه أفرز تحديات معقدة، خاصة في مجال الأمن المعلوماتي، حيث:

- أصبحت المكتبات تعتمد بشكل شبه كلي على الأنظمة الرقمية

• تزايدت كميات البيانات الحساسة (بيانات المستخدمين، سجلات البحث)

• ارتبطت الخدمات بشبكات مفتوحة (الإنترنت)

• مما جعلها عرضة لمجموعة من التهديدات، مثل:

• الهجمات السيبرانية

• اختراق الأنظمة

• تسريب البيانات

• فقدان المعلومات

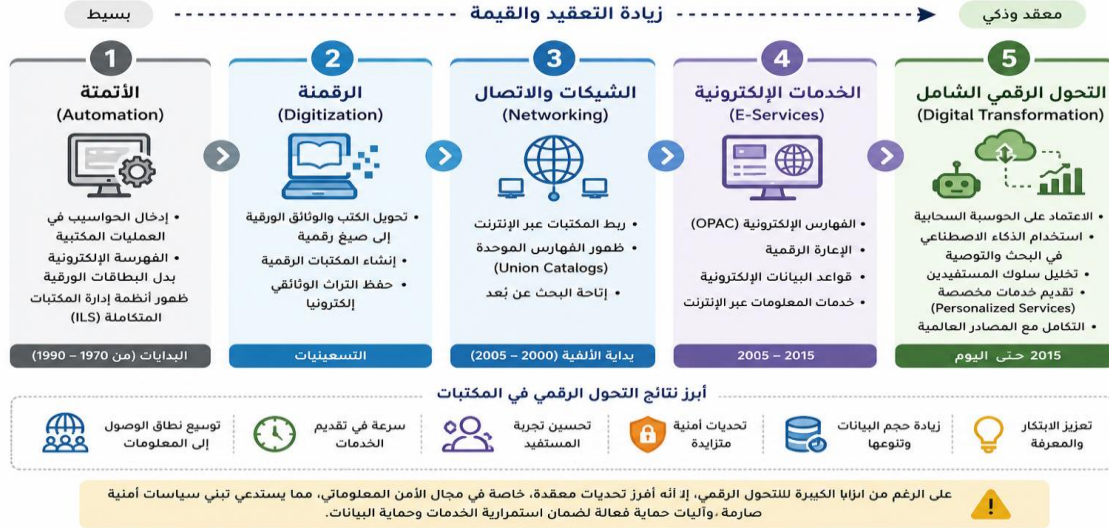
ويؤكد (Tenopir et al., 2012) أن التحول نحو البيئة الرقمية، رغم فوائده، "يزيد من تعقيد إدارة

المعلومات ويطرح تحديات أمنية جديدة تتطلب استراتيجيات متقدمة للحماية."

يتضح أن التحول الرقمي لم يكن مجرد تحديث تقني، بل هو تحول بنيوي شامل أعاد تعريف وظيفة المكتبة ودورها في المجتمع المعرفي. غير أن هذا التحول يفرض في المقابل ضرورة تبني سياسات أمنية صارمة وآليات حماية فعالة لضمان استمرارية الخدمات وحماية البيانات، مما يجعل الأمن السيبراني عنصراً لا ينفصل عن بيئة المكتبات الحديثة.

مراحل التحول الرقمي في المكتبات

من الأتمتة إلى التحول الرقمي الشامل



الشكل رقم 1: يبين التحول الرقمي في المكتبات (بتصرف)

3. التهديدات السيبرانية في المكتبات

في ظل التحول الرقمي المتسارع واعتماد مؤسسات المعلومات على الحوسبة السحابية والنظم الآلية المتكاملة (ILS)، لم تعد المكتبات مجرد مستودعات هادئة للكتب، بل أصبحت قواعد بيانات ضخمة تحتوي على أصول رقمية قيمة ومعلومات حساسة. هذا التحول جعلها أهدافاً استراتيجية لمجرمي الإنترنت. يمكن تصنيف أبرز التهديدات السيبرانية التي تواجهها المكتبات إلى المحاور التالية:

1.3 الهجمات الإلكترونية

تتعرض المكتبات لأنواع متعددة وموجهة من الهجمات الإلكترونية التي تهدف إلى شل حركتها أو استغلال مواردها. وتتنوع هذه الهجمات لتشمل:

- **الاختراق:** حيث يحاول المهاجمون استغلال الثغرات الأمنية للوصول غير المصرح به إلى الأنظمة الداخلية، سواء لتخريب الفهارس أو للوصول إلى الخوادم الرئيسية للمؤسسة الأم (كالجامعة أو الوزارة).
- **الفيروسات والبرمجيات الخبيثة:** والتي تنتقل عادة عبر شبكات الإنترنت اللاسلكية العامة المفتوحة التي توفرها المكتبات لروادها، مما يؤدي إلى تلف البيانات أو تعطيل أجهزة الكمبيوتر العامة.
- **هجمات الفدية الخبيثة:** وتُعد من أشرس التهديدات المعاصرة وأكثرها تدميراً. في هذا السيناريو، يقوم القراصنة بتشفير قواعد بيانات المكتبة (بما في ذلك الفهارس، المستودعات الرقمية، وبيانات المستفيدين) ويطالبون بدفع مبالغ مالية ضخمة (غالباً بالعملات المشفرة) مقابل مفتاح فك التشفير. وتشير تقارير الوكالة الأوروبية للأمن السيبراني إلى تزايد ملحوظ في استهداف المؤسسات التعليمية والمكتبات نظراً لضعف ميزانيات الحماية المخصصة لها مقارنة بالقطاعين المالي والصحي. (ENISA, 2023)

من أبرز الأمثلة وأحدثها ما تعرضت له المكتبة البريطانية (*The British Library*) في أكتوبر 2023، حيث تعرضت لهجوم فدية مدمر من قبل مجموعة تُدعى (*Rhysida*) أدى الهجوم إلى شلل كامل في الموقع الإلكتروني للمكتبة، وتعطل الفهرس العام للجمهور (*OPAC*)، وتوقف خدمات الإعارة الرقمية لأشهر طويلة، مما كبد المكتبة خسائر مالية فادحة لإعادة بناء أنظمتها. (*British Library, 2024*) وفي نفس العام، تعرضت مكتبة تورونتو العامة (*Toronto Public Library*) في كندا لهجوم مشابه أدى إلى تعطيل الحواسيب العامة وخدمات الطباعة وسرقة بيانات حساسة للموظفين. (*ALA, 2023*)

2.3 تسريب البيانات:

تعتبر حماية خصوصية المستفيدين من أقدم أخلاقيات مهنة المكتبات، يُعد تسريب البيانات اختراقاً كارثياً لهذا المبدأ، حيث يؤدي إلى كشف معلومات شخصية وحساسة مثل الأسماء، العناوين، سجلات الإعارة، والاهتمامات البحثية، هذا التسريب قد يحدث نتيجة هجمات اختراق معقدة، أو بسبب ثغرات في أنظمة الموردين الخارجيين، أو حتى نتيجة أخطاء بشرية غير مقصودة من قبل موظفي المكتبة (كفتح رسائل تصيد احتيالي) خطورة هذا التسريب تكمن في إمكانية استخدام بيانات المستفيدين في عمليات ابتزاز أو بيعها في الويب المظلم (*Dark Web*).

في عام 2020، تعرضت شركة بلاكباود — (*Blackbaud*) وهي مزود رئيسي لبرمجيات إدارة قواعد البيانات السحابية التي تستخدمها مئات المكتبات الجامعية والمؤسسات غير الربحية حول العالم — لاختراق هائل أدى إلى تسريب بيانات ملايين المستخدمين والمانحين والباحثين المسجلين في تلك المكتبات. هذا الحادث دفع ناقوس الخطر حول مخاطر الاعتماد على مزودي الخدمات السحابية دون التدقيق في بروتوكولاتهم الأمنية (*EDUCAUSE, 2021*).

3. 4. ضعف البنية التحتية التقنية

تعاني العديد من مؤسسات المعلومات، ولا سيما في الدول النامية وفي المكتبات العامة أو المدرسية ذات الميزانيات المحدودة، من فجوات خطيرة في البنية التحتية التقنية. يتمثل هذا الضعف في:

- أنظمة قديمة غير محدّثة: استمرار الاعتماد على أنظمة تشغيل انتهى دعمها الفني (مثل إصدارات ويندوز القديمة) أو نظم إدارة مكتبات لم تعد تتلقى تحديثات أمنية.
- نقص في برامج الحماية المتطورة: غياب أنظمة الكشف عن التسلل أو جدران الحماية المتقدمة.
- الافتقار للكادر البشري المتخصص: عدم وجود أخصائيي أمن معلومات متفرغين داخل المكتبات، والاعتماد الكلي على أقسام تكنولوجيا المعلومات المركزية التي قد تتأخر في الاستجابة، هذه الهشاشة التقنية تجعل من المكتبات "الحلقة الأضعف" والهدف الأسهل لمجرمي الإنترنت.

أشار تقرير للاتحاد الدولي لجمعيات ومؤسسات المكتبات (IFLA, 2022) إلى أن العديد من المكتبات العامة في إفريقيا وأمريكا اللاتينية تفتقر إلى سياسات أساسية لأمن المعلومات، حيث تعتمد حواسيب إعاره الجمهور على برمجيات غير أصلية أو منتهية الصلاحية، مما جعل بعضها يقع ضحية سهولة لفيروسات الفدية القديمة مثل (WannaCry)، والتي انتشرت في شبكاتها الداخلية ببساطة بسبب غياب التحديثات الأمنية الدورية وغياب النسخ الاحتياطي السحابي للأمن.

4. آليات حماية البيانات في مؤسسات المعلومات

أمام التهديدات السيبرانية المتزايدة، لم يعد بناء استراتيجية أمنية قوية خياراً ترفيهياً للمكتبات، بل أصبح حتمية مهنية وقانونية لضمان استمرارية الخدمات وحماية خصوصية المستفيدين، وتعتمد هذه الاستراتيجية على منظومة متكاملة من الآليات التقنية والإدارية، أبرزها:

1.4 التشفير (Encryption)

يُعد التشفير حجر الزاوية في حماية البيانات الرقمية. وتعتمد فكرته على استخدام خوارزميات رياضية معقدة لتحويل المعلومات إلى نصوص مُعمّاة غير قابلة للقراءة، ولا يمكن إعادتها لحالتها الأصلية إلا عبر "مفتاح تشفير" يمتلكه المستخدم المصرح له فقط. في البيئة المكتبية، يُطبق التشفير على مستويين رئيسيين: الأول هو "تشفير البيانات في حالة السكون"، والذي يُستخدم لحماية قواعد البيانات وسجلات المستفيدين المخزنة على خوادم المكتبة؛ والثاني هو "تشفير البيانات أثناء النقل"، والذي يؤمن الاتصالات بين حاسوب المستفيد وخوادم الفهرس الآلي (OPAC) لمنع اعتراض البيانات أثناء تصفح شبكة الإنترنت، ويتم ذلك عادة عبر بروتوكولات آمنة مثل (HTTPS) و (SSL/TLS). كما يُستخدم التشفير بشكل قياسي لحماية كلمات المرور الخاصة بالموظفين والمستفيدين باستخدام تقنيات "التجزئة" (Hashing) " لمنع كشفها حتى في حال اختراق قاعدة البيانات. (Stallings, 2017)

2.4 أنظمة الحماية والمراقبة الشبكية

لا يمكن للمكتبة أن تترك شبكتها الداخلية مشرعة أمام شبكة الإنترنت العامة دون بوابات حراسة إلكترونية. تتشكل هذه الحراسة من طبقتين دفاعيتين:

• الجدران النارية: (**Firewalls**) تمثل خط الدفاع الأول؛ فهي برمجيات أو أجهزة صلبة تراقب حركة المرور الشبكية (الداخلية والخارجية)، وتعمل كعازل بين شبكة المكتبة الداخلية الموثوقة وشبكة الإنترنت الخارجية، مانعة أي اتصال غير مصرح به بناءً على قواعد أمنية محددة مسبقاً.

• أنظمة كشف ومنع التسلل: (**IDS/IPS**) تعمل ككاميرات المراقبة المتقدمة داخل الشبكة. تقوم هذه الأنظمة بتحليل حزم البيانات (**Packets**) لرصد أي أنماط غير طبيعية أو أنشطة مشبوهة قد تدل على محاولة اختراق، وتقوم بإرسال تنبيهات فورية للمسؤولين، وفي حالة أنظمة المنع (**IPS**)، تتدخل آلياً لإيقاف الهجوم. وتُعد هذه الأنظمة بالغة الأهمية للمكتبات الجامعية التي تتعرض لمحاولات اختراق متكررة لسرقة الأبحاث (**Bace & Mell, 2001**).

3.4 إدارة الهوية وإمكانية الوصول

تُركز هذه الآلية على مبدأ "أمن الثقة المعدومة" (**Zero Trust**) "فالتهديد لا يأتي دائماً من الخارج، بل قد ينبع من أخطاء داخلية. يهدف نظام (**IAM**) إلى التأكد من هوية المستخدمين وتحديد ما يحق لهم القيام به داخل النظام الآلي للمكتبة. (**ILS**) وتعتمد هذه الإدارة على:

• التحكم في الصلاحيات: (**Role-Based Access Control**) حيث لا يُمنح جميع موظفي المكتبة نفس الحقوق؛ فصلاحيات "موظف الإعارة" تختلف عن صلاحيات "مدير النظام" الذي يمتلك حق التعديل على قاعدة البيانات بأكملها.

• المصادقة متعددة العوامل: (**MFA**) وهي تقنية حيوية لمنع الاستخدام غير المشروع، حيث لا يُكتفى بكلمة المرور فقط للدخول إلى الأنظمة الحساسة، بل يُطلب من الموظف إثبات هويته بعامل آخر، مثل رمز يُرسل إلى هاتفه المحمول أو بصمة بيومترية. وقد أثبتت الدراسات أن تطبيق الـ (**MFA**) يقلل من نجاح هجمات اختراق الحسابات بنسبة تتجاوز 90% (**Microsoft, 2022**).

4.4 النسخ الاحتياطي وخطة التعافي من الكوارث (**Backup & Disaster Recovery**)

مهما بلغت قوة أنظمة الحماية، يبقى احتمال الاختراق وارداً. هنا يبرز دور "النسخ الاحتياطي" كخط الدفاع الأخير وطوق النجاة الحقيقي، لاسيما في مواجهة هجمات برمجيات الفدية (**Ransomware**) التي تُسفر بيانات المكتبة بالكامل. لكي يكون النسخ الاحتياطي فعالاً، يجب أن يخضع لقاعدة (3-2-1) الأمنية الشهيرة؛ أي الاحتفاظ بثلاث نسخ من البيانات، على وسيطي تخزين مختلفين (مثل أقراص صلبة خارجية وخوادم محلية)، مع وضع نسخة واحدة على الأقل خارج مقر المكتبة (**Off-site**) كالتخزين السحابي الآمن، يجب أن تكون هذه العملية دورية ومؤتمنة، محفوظة في بيئة معزولة عن الشبكة الرئيسية لمنع انتقال الفيروسات إليها، ومصممة بحيث تكون قابلة للاسترجاع بسرعة لضمان عودة خدمات المكتبة للعمل في أسرع وقت وتقليل فترات التوقف (**Brooks et al., 2018**).

5. دور السياسات والتشريعات في حوكمة البيانات

لا يمكن للحلول التقنية (مثل التشفير والجدران النارية) أن تحقق أماناً شاملاً بمعزل عن إطار حوكمة تنظيمي يحدد كيفية التعامل مع المعلومات. لذا، تبرز أهمية السياسات والتشريعات كدرع قانوني وأخلاقي يضبط

حركة البيانات داخل مؤسسات المعلومات، ويضمن عدم المساس بحقوق المستفيدين. وينقسم هذا المحور إلى بُعدين متكاملين: قانوني وأخلاقي.

1.5 قوانين حماية البيانات:

أصبحت التشريعات الوطنية والدولية تلعب دوراً محورياً في رسم خارطة طريق إلزامية لحماية البيانات الرقمية. لم تعد مسألة تأمين الأنظمة خياراً داخلياً للمكتبة، بل أصبحت التزاماً قانونياً يحاسب عليه القانون. تركز هذه التشريعات على تقنين "دورة حياة البيانات"، بدءاً من:

- تنظيم آليات الجمع والاستخدام: حيث تُلزم القوانين المكتبات بجمع الحد الأدنى من البيانات الضرورية لتقديم الخدمة (**Data Minimization**)، واشتراط الحصول على "موافقة صريحة من المستفيد قبل تخزين بياناته الشخصية أو استخدامها لأغراض إحصائية.

- إلزام المؤسسات بمعايير الأمان التقنية: تفرض هذه القوانين على المؤسسات تبني أقصى درجات الحماية وتطبيق معايير أمان معتمدة مثل سلسلة (**ISO 27001**)، مع إلزامها بالتبليغ الفوري للجهات المختصة وللمستفيدين في حال حدوث أي تسريب أو اختراق للبيانات.

وقد أثبتت الدراسات التقييمية أن الامتثال الصارم لهذه التشريعات ينعكس إيجاباً على البنية الأمنية للمؤسسات، حيث يُقلل بشكل ملحوظ من مخاطر الاختراقات والهجمات السيبرانية نتيجة التحديث المستمر

للسياسات الدفاعية. (Greenleaf, 2022)

مثال واقعي: يُعد اللائحة العامة لحماية البيانات (**GDPR**) التي أقرها الاتحاد الأوروبي عام 2018، من أبرز الأمثلة في هذا السياق. لقد أحدث هذا القانون زلزالاً إيجابياً في قطاع المكتبات الأوروبية وحتى العالمية، حيث أُجبرت المكتبات على مراجعة سياسات الفهارس الآلية (**OPAC**)، وأصبحت ملزمة قانونياً بحذف سجلات استعارة المستفيدين بمجرد إرجاع الكتب، لضمان عدم تتبع اهتماماتهم القرائية، فضلاً عن منح المستفيد حق "النسيان" أو محو بياناته من خوادم المكتبة نهائياً. (Voigt & Von dem Bussche, 2017)

2.5 أخلاقيات استخدام المعلومات:

تمتد مسؤولية المكتبات إلى بُعد أعمق من مجرد الامتثال القانوني الصرف، وهو "البُعد الأخلاقي". فتاريخياً، بُنيت مهنة المكتبات على قيم جوهرية تتمحور حول ثقة المستفيد، وهو ما يفرض على أخصائيي المعلومات مسؤولية أخلاقية تتجلى في:

- حماية خصوصية المستخدمين (**User Privacy**): يُعتبر ما يقرأه المستفيد أو يبحث عنه شأنًا خاصاً لا يجوز مراقبته أو تتبعه.

- ضمان حرية الوصول دون رقابة: يجب أن تكون المكتبة مساحة آمنة فكرياً، تُتيح للمستفيد البحث في مختلف الموضوعات دون خوف من تسجيل نشاطه أو تسليمه لجهات خارجية رقابية.

- عدم إساءة استخدام البيانات: مع تزايد استخدام أنظمة "تحليلات البيانات الضخمة" (**Big Data**)

(**Analytics**) لتحسين خدمات المكتبة، تواجه المؤسسات معضلة أخلاقية؛ فبرغم أن تحليل سلوك المستخدمين يساعد في تطوير المجموعات المكتبية، إلا أنه قد ينتهك خصوصيتهم إذا تم استخدامه كأداة للمراقبة التجارية أو بيع البيانات لجهات خارجية.

لذا، يفرض هذا الواقع التزاماً مهنيًا دقيقاً بخلق "توازن حرج" بين الانفتاح (*Openness*) وتقديم خدمات مخصصة من جهة، وبين الحماية المطلقة للخصوصية من جهة أخرى. (*Zimmer, 2013*) مثال واقعي: يتجلى هذا الالتزام الأخلاقي بوضوح في موقف جمعية المكتبات الأمريكية (*ALA*) وإعلانها الشهير لميثاق الشرف المهني. ففي أعقاب صدور "قانون باتريوت (*Patriot Act*)" الأمريكي الذي سمح للأجهزة الأمنية بالوصول إلى سجلات رواد المكتبات، قادت المكتبات حركة أخلاقية مضادة، حيث قامت ببرمجة أنظمتها الآلية لتمسح سجلات الإعارة والبحث للمستفيدين بشكل آلي ويومي. (*Data Purging*) هذا الإجراء لم يكن مدفوعاً بضعف تقني، بل بقرار أخلاقي لمنع أي جهة، حكومية أو تجارية، من استغلال بيانات المستفيدين واستخدامها ضدهم.

6. التحديات التي تواجه المكتبات الحديثة في البيئة الرقمية

إن مساعي مؤسسات المعلومات لتحقيق بيئة سيبرانية آمنة ومستقرة لا تخلو من العقبات؛ إذ تصطدم هذه المؤسسات بواقع إداري وتقني يفرض جملة من التحديات الهيكلية التي تحد من كفاءة استجابتها للتهديدات. يمكن بلورة أبرز هذه التحديات في المحاور الثلاثة الآتية:

1.6 نقص الموارد المالية والبشرية:

تُصنف المكتبات — في الغالب — ضمن المؤسسات الخدمية غير الربحية، مما يجعلها عرضة دائمة لسياسات التقشف واقتطاع الميزانيات. هذا القصور المالي ينعكس بشكل مباشر وخطير على بنيتها الأمنية من زاويتين:

• العجز عن مواكبة البنية التحتية: تتطلب الحماية الفعالة استثمارات مالية ضخمة لشراء وتحديث أنظمة الحماية المتطورة (مثل الجدران النارية من الجيل القادم، وأنظمة التشفير المعقدة، والاشتراكات في الخدمات السحابية الآمنة). ومحدودية الميزانية تجبر المكتبات على الاكتفاء بالحلول الأمنية الأساسية أو المجانية التي لا توفر تغطية شاملة.

• صعوبة استقطاب الكفاءات: يشهد سوق العمل العالمي تنافساً شرساً على خبراء أمن المعلومات، ونظراً لارتفاع أجور هؤلاء المتخصصين في القطاع الخاص والتجاري، تعجز المكتبات عن توظيف كوادر أمنية متفرغة، وتضطر للاعتماد على أقسام الدعم التقني العام التي قد تفتقر للتخصص الدقيق في التصدي للهجمات المعقدة. (*Breeding, 2021*)

2.6 الفجوة في التكوين التقني والوعي الأمني

تؤكد أدبيات أمن المعلومات أن "العنصر البشري هو الحلقة الأضعف" في أي سلسلة دفاعية، في البيئة المكتبية، يتمحور التكوين الأكاديمي لأخصائيي المعلومات حول تنظيم المعرفة واسترجاعها، وغالباً ما يفتقرون إلى التدريب المتعمق في بروتوكولات الأمن السيبراني. هذا النقص في التكوين المستمر والوعي الأمني يؤدي إلى تفاقم "الأخطاء البشرية"؛ حيث يصبح الموظفون عرضة لأساليب الهندسة الاجتماعية ورسائل التصيد الاحتيالي، مما قد يمنح المهاجمين وصولاً غير مصرح به للأنظمة الداخلية بمجرد نقرة خاطئة من موظف غير مدرب، مهما بلغت قوة البرمجيات الدفاعية المتبناة. (*Hadlington, 2017*)

3.6 التطور المتسارع والمعد للتهديدات السيبرانية

تتسم البيئة السيبرانية بديناميكية عالية، حيث يبتكر قراصنة الإنترنت باستمرار تقنيات هجومية جديدة تتجاوز الدفاعات التقليدية (مثل هجمات "اليوم الصفر" أو **Zero-Day Exploits**)، واستخدام الذكاء الاصطناعي في الهجوم (الآلي). في المقابل، تتسم البيئة الإدارية للمكتبات بالبطء النسبي في اتخاذ القرار وتحديث السياسات. هذا التباين يخلق فجوة زمنية خطيرة؛ فالتطور السريع للتهديدات يجعل من الصعب جداً على المكتبات مواكبتها دون وجود استراتيجية استباقية وتحديث فوري ودائم للأنظمة الآلية وخوادم الفهارس. عدم القدرة على المزامنة السريعة مع هذه التهديدات المستحدثة يبقي المكتبة في حالة "رد الفعل" المتأخر بدلاً من "الوقاية" الاستباقية. (Kshetri, 2021)

خاتمة:

تخلص هذه الدراسة إلى حقيقة جوهرية مفادها أن الأمن السيبراني قد تجاوز مرحلة كونه إجراءً تقنياً تكميلياً، ليصبح ركيزة استراتيجية وحتمية مؤسساتية تضمن استمرارية مؤسسات المعلومات الحديثة وتصور موثوقيتها. لقد أثبت التحليل المنهجي للواقع التقني أن التحول الرقمي المتسارع، ورقمنة الأرصدة الوثائقية، والاعتماد المتزايد على الحوسبة السحابية والنظم الآلية المتكاملة (ILS)، قد وضع المكتبات في الخطوط الأمامية لمواجهة بيئة سيبرانية شديدة التعقيد والعدائية. وقد أبرزت الدراسة أن المخاطر التي تواجهها المكتبات لم تعد تقتصر على الأعطال التقنية البسيطة، بل اتسعت لتشمل هجمات سيبرانية موجهة وخطيرة، كبرمجيات الفدية (**Ransomware**) وعمليات الاختراق المنهجي التي تهدف إلى سرقة الأصول الرقمية وتسريب البيانات الحساسة للمستخدمين. وفي المقابل، أظهرت المقاربة التحليلية أن الهشاشة الأمنية لا تنبع فقط من قوة المهاجمين، بل تتجذر أحياناً في ضعف البنية التحتية الداخلية، وقصور الميزانيات المخصصة للتأمين التكنولوجي، فضلاً عن كون "العنصر البشري" غير المدرب يمثل الثغرة الأكبر في أي منظومة دفاعية. كما توصلت الدراسة إلى أن تحقيق أمن معلوماتي رصين ومستدام لا يمكن أن يعتمد حصراً على الحلول البرمجية الجاهزة — كالتشفير والجدران النارية — بل يستدعي مقاربة "شمولية متكاملة" (**Holistic Approach**). هذه المقاربة تدمج بين الحصانة التقنية، والحوكمة الإدارية عبر سياسات داخلية صارمة، والامتثال الصارم للتشريعات القانونية المنظمة لخصوصية البيانات، إلى جانب الالتزام الأخلاقي الذي يُعد صمام الأمان لرسالة المكتبة.

وعليه، فإن بقاء المكتبات كمؤسسات موثوقة وحاضنة للابتكار في مجتمع المعرفة الرقمي، مرهون بمدى قدرتها على التكيف الاستباقي. يتطلب هذا التكيف الانتقال من عقلية "رد الفعل" بعد وقوع الكارثة، إلى عقلية "إدارة المخاطر الوقائية" (**Proactive Risk Management**)، عبر الاستثمار الاستراتيجي في الأنظمة والأفراد على حد سواء، لتحقيق تلك المعادلة الصعبة والضرورية: الحفاظ على تدفق المعلومات وإتاحتها بحرية، مع ضمان أعلى درجات الحماية والسرية للبيانات.

التوصيات



بناءً على الاستنتاجات التحليلية التي أفرزتها هذه الدراسة، وفي سبيل بناء بيئة معلوماتية آمنة ومستدامة، نقترح التوصيات المنهجية التالية لمسيرى المكتبات وصناع القرار:

أولاً: على مستوى المورد البشري وبناء القدرات

- تأسيس برامج تكوين مستمر :إخضاع جميع العاملين في المكتبة (بغض النظر عن درجاتهم الوظيفية) لبرامج تدريبية دورية ومتخصصة في الوعي الأمني ، لتمكينهم من التعرف على أساليب الهندسة الاجتماعية ورسائل التصيد الاحتيالي، وتحويلهم من "نقطة ضعف" إلى "خط دفاع أول".
- نشر الثقافة الأمنية بين المستفيدين :إطلاق حملات توعوية لرواد المكتبة حول كيفية الاستخدام الآمن لشبكات المكتبة العامة والمنصات الرقمية التابعة لها، وأهمية حماية بيانات الدخول الخاصة بهم.

ثانياً: على مستوى البنية التحتية والحلول التقنية

- الاستثمار المالي في البنية التحتية الرقمية :تخصيص بند مالي ثابت وكافٍ ضمن الميزانية السنوية للمكتبة لتحديث الخوادم، واقتناء برمجيات حماية متقدمة كأنظمة كشف التسلل (IDS)، والانتقال إلى بيئات التخزين السحابية الموثوقة.
- تطبيق سياسة التحديث الآلي والدوري : (Patch Management) الالتزام بالتحديث الفوري والدائم لنظم إدارة المكتبات (LMS) وأنظمة التشغيل لسد الثغرات الأمنية (Zero-day vulnerabilities) التي قد يستغلها القراصنة.

ثالثاً: على مستوى الحوكمة والتشريعات المؤسسية

- صياغة واعتماد سياسات أمن معلومات شاملة :إعداد وثائق رسمية واضحة تحدد بروتوكولات حماية البيانات، وآليات التحكم في الصلاحيات (Access Control) ، وخطة استجابة فورية للحوادث السيبرانية لضمان التعافي السريع وتقليل الخسائر في حال وقوع هجوم.
- إعادة هندسة أنظمة النسخ الاحتياطي :تبني استراتيجيات نسخ احتياطي معزولة ومؤتمتة (مثل قاعدة 3-2-1)، لضمان استرجاع البيانات بأمان تام بعد أي هجوم فدية.

رابعاً: على مستوى التعاون المؤسسي

- بناء شراكات استراتيجية :الانخراط الفاعل مع المؤسسات الحكومية والخاصة المتخصصة في الأمن السيبراني، ومراكز الاستجابة لطوارئ الحاسب الآلي، لتبادل التنبيهات الأمنية المبكرة، والخبرات، وأفضل الممارسات لحماية الموارد الوثائقية.
- وفي الختام، لا تدّعي هذه الدراسة الإحاطة المطلقة بكافة تعقيدات المشهد السيبراني المتشابك في قطاع المكتبات، بل تمثل لبنة تأسيسية تفتح آفاقاً رحبة أمام مسارات بحثية مستقبلية أكثر تخصصاً وعمقاً، إن التطور المتسارع للتقنيات الناشئة يفرض على الباحثين ضرورة استكشاف آفاق متجددة، كدراسة دور تقنيات الذكاء الاصطناعي (AI) وتعلم الآلة في التنبؤ الاستباقي بالهجمات السيبرانية داخل نظم إدارة المكتبات، أو تقييم فاعلية تقنية "البلوكتشين (Blockchain)" في توثيق وحماية الأرشيفات الرقمية من التلاعب. كما تبرز الحاجة الماسة لإجراء دراسات ميدانية وسلوكية ترصد السيكلوجية الأمنية لرواد المكتبات وموظفيها للحد من ثغرات "الهندسة الاجتماعية". وبهذا المعنى، يبقى النقاش الأكاديمي في هذا الحقل الحيوي مفتوحاً وديناميكياً، أملاً في بناء إطار معرفي وتطبيقي شامل يُحصّن ذاكرة المجتمع ومؤسساته الثقافية ضد تقلبات وتحديات العصر الرقمي اللامتناهية.

قائمة المراجع:

1. قاسم، محمد (2018) المكتبات الرقمية وتحديات العصر. دار المسيرة، عمان.
2. المنظمة العربية لتكنولوجيات الاتصال والمعلومات. (2019) دليل الأمن السيبراني العربي. تونس.
3. Alshammari, M., & Simpson, A. (2017). Towards a principled approach for engineering privacy by design. *Journal of Information Security and Applications*, 36, 62–76.
4. American Library Association (ALA). (2023). *Cybersecurity and public libraries: Lessons learned from the Toronto Public Library attack*. Chicago: ALA Editions.
5. Bace, R., & Mell, P. (2001). *Intrusion detection systems*. NIST Special Publication 800-31. National Institute of Standards and Technology.
6. British Library. (2024). *Learning lessons from the cyber-attack*. The British Library Official Reports. Retrieved from the British Library Policy & Strategy archives
7. Borgman, C. L. (2000). *From Gutenberg to the Global Information Infrastructure*. MIT Press.
8. Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Sybex.
9. EDUCAUSE. (2021). *The ripple effect of the Blackbaud data breach on higher education and library institutions*. EDUCAUSE Review.
10. European Union Agency for Cybersecurity (ENISA). (2023). *Threat landscape for the education and research sector*. Athens: ENISA Publications.
11. European Union. (2016). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union.
12. Greenleaf, G. (2022). *Global data privacy laws: 2022 and beyond*. *Privacy Laws & Business International Report*, 175, 1-6.
13. International Federation of Library Associations and Institutions (IFLA). (2022). *Digital infrastructure and cybersecurity in developing libraries: A global report*. The Hague: IFLA Headquarters.
14. ISO (2012). *ISO/IEC 27032: Guidelines for cybersecurity*. International Organization for Standardization.
15. ITU (2018). *Overview of cybersecurity*. International Telecommunication Union.
16. Kshetri, N. (2021). *Cybersecurity Management: An Organizational and Strategic Approach*. University of Toronto Press.
17. Microsoft. (2022). *Microsoft digital defense report 2022*. Redmond: Microsoft Corporation.
18. NIST (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.
19. Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards*. Auerbach Publications.

20. Stallings, W. (2017). *Cryptography and network security: Principles and practice (7th ed.)*. Pearson.
21. Tenopir, C., et al. (2012). *Academic Libraries and Research Data Services*. Association of College & Research Libraries.
22. Von Solms, R., & Van Niekerk, J. (2013). *From information security to cybersecurity*. *Computers & Security*, 38, 97–102.
23. Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide (1st ed.)*. Springer International Publishing.
24. Zimmer, M. (2013). *Assessing the treatment of patron privacy in library 2.0 literature*. *Information Technology and Libraries*, 32(2), 29-41.