مقالات (الملخص العربي)
https://doi.org/10.70000/cj.2026.78.760

تحديات خصوصية وأمن بيانات المستفيدين في المكتبات الرقمية: مراجعة للإنتاج الفكري

عمر حسن عبد الرحمن [1]

[1] جامعة الخرطوم، قسم علوم المكتبات والمعلومات، السودان

omerhassanab@gmail.com

بيانات المقال

التاريخ
الإستلام: 08.08.2025
القبول: 11.03.2026
النشر: 29.04.2026

الكلمات المفتاحية
المكتبات الرقمية، خصوصية البيانات، أمن المعلومات، الذكاء الإصطناعي، مراجعة الإنتاج الفكري

المستخلص

تُعد المكتبات الرقمية ركيزة أساسية للبحث والتعلم في العصر الحديث، حيث وسعت التطورات التقنية نطاق وصولها العالمي. ومع ذلك، أدى هذا التوسع إلى زيادة جمع ومعالجة بيانات المستخدمين لتقديم تجارب مخصصة، مما أثار مخاوف حرجة بشأن الخصوصية والأمن. تسلط هذه الوثيقة الضوء على التوازن المعقد بين الاستفادة من البيانات لتحسين الخدمات وبين حمايتها من التهديدات المتزايدة. تشير النتائج إلى أن الهجمات السيبرانية، مثل برامج الفدية واختراقات البيانات، لم تعد مجرد احتمالات بل واقعاً واجهته مؤسسات كبرى مثل المكتبة البريطانية وأرشيف الإنترنت. يتطلب تأمين هذه البيانات نهجاً متعدد الأبعاد يشمل التدابير التقنية، والامتثال التنظيمي، مثل لائحة GDPR، وتبني "الخصوصية بالتصميم" كمعيار أساسي، خاصة مع دمج التقنيات الناشئة مثل الذكاء الاصطناعي وسلسلة الكتل (Blockchain).

1. أنواع بيانات المستخدمين المجموعة في المكتبات الرقمية

تجمع المكتبات الرقمية أنواعاً مختلفة من البيانات لتحليل سلوك المستخدمين وتحسين جودة الخدمات المقدمة:

- بيانات الاستخدام وسجلات النشاط :تشمل سجل البحث، عدد المشاهدات والتحميلات، مدة الجلسات، طوابع تسجيل الدخول والخروج، وتقارير الأخطاء.
- البيانات التقنية :عناوينIP ، نوع المتصفح وإصداره، نظام التشغيل، أنواع الأجهزة المستخدمة، ومصادر الإحالة.
- بيانات الحساب والمصادقة :أسماء المستخدمين، وثائق الهوية، عناوين البريد الإلكتروني، البيانات الديموغرافية، وحالة العضوية.
- بيانات التخصيص :عادات القراءة وتفضيلات المحتوى.

2. انتهاكات الخصوصية والتهديدات الأمنية

تُعرف "الخصوصية" في هذا السياق بقدرة المستخدم على التحكم في كيفية الوصول إلى بياناته وإدارتها ومشاركتها. وتواجه هذه الخصوصية تهديدات متنوعة:

أ. الهجمات السيبرانية واختراقات البيانات

تستهدف الهجمات السيبرانية الوصول غير المصرح به لسرقة المعلومات الشخصية عبر طرق متطورة:

- اختراقات البيانات :(Data Breaches) الوصول غير القانوني لقواعد البيانات الحساسة، مما يؤدي لسرقة الهوية.
- البرامج الضارة :(Malware) تثبيت برمجيات تخريبية لتعطيل وظائف المكتبة.
- التصيد الاحتيالي :(Phishing) خداع الموظفين أو المستخدمين للكشف عن بيانات الاعتماد.
- هجمات حجب الخدمة :(DDoS) إغراق خوادم المكتبة بحركة مرور كثيفة لتعطيل الخدمات.
- التهديدات الداخلية :استغلال الأفراد داخل المنظمة لصلاحياتهم للوصول إلى البيانات أو التلاعب بها.

ب. مشاركة البيانات مع أطراف ثالثة

- دمج أدوات الطرف الثالث :قد تقوم تقنيات مثل تحليلات البيانات الضخمة أو مزودي المصادقة بجمع بيانات تتجاوز سيطرة المكتبة، أحياناً لأغراض إعلانية.
- نقص الشفافية مع الموردين :غالباً ما تفتقر المكتبات للمعرفة الكافية حول كيفية إدارة الموردين لبيانات مستخدميها.

ج. السياسات والممارسات غير الكافية

- فشل العديد من المكتبات في الإفصاح الصريح عن كيفية استخدام البيانات أو الامتثال للوائح القانونية، بالإضافة إلى ضعف السياسات المتعلقة بتقنيات "إنترنت الأشياء."

3. تداعيات الانتهاكات الأمنية

تؤدي انتهاكات البيانات إلى عواقب وخيمة تؤثر على المؤسسة والمستخدم على حد سواء:

1. فقدان الثقة :تراجع استخدام خدمات المكتبة عندما يشعر المستخدمون بأن بياناتهم مراقبة أو معرضة للخطر.
2. سرقة الهوية والاحتيال المالي :الضرر المباشر للأفراد نتيجة تسريب معلوماتهم الحساسة.
3. "تأثير التجميد" على حرية التعبير :قد يؤدي الشعور بالرقابة إلى الرقابة الذاتية للمستخدمين، مما يضر بالديمقراطية والمشاركة المدنية.
4. العواقب القانونية والمالية :تشمل الغرامات الباهظة الناتجة عن عدم الامتثال للوائح، والدعاوى القضائية من المتضررين، وتكاليف التعافي من الاختراق.
5. تعطيل العمليات :شلل سير العمل وجعل الوثائق غير متاحة للمستخدمين الشرعيين.

4. أفضل الممارسات لحماية البيانات والخصوصية

لحماية بيانات المستخدمين، يجب على المكتبات الرقمية تبني إطار عمل شامل:

التدابير التقنية والسياساتية

النوع	الإجراءات المقترحة
التدابير التقنية	التشفير (للبيانات المخزنة والمنتقلة)، المصادقة متعددة العوامل(MFA) ، التحديثات الدورية للبرمجيات، والمراقبة الأمنية المستمرة.
التدابير السياساتية	الشفافية في سياسات البيانات، تبني نهج "الخصوصية بالتصميم" (جعل الخصوصية الإعداد الافتراضي)، واتفاقيات واضحة لمشاركة البيانات مع الأطراف الثالثة.
التدابير التنظيمية	تدريب الموظفين على الوعي الأمني، ووضع خطة استجابة للحوادث تم اختبارها مسبقاً.

الامتثال التنظيمي GDPR

تعتبر اللائحة العامة لحماية البيانات (GDPR) معياراً عالمياً يتطلب:

- الحصول على الموافقة :لجمع البيانات الشخصية.
- تقليل البيانات :جمع ما هو ضروري فقط لغرض محدد.
- حقوق الأفراد :الحق في المعرفة، والاعتراض، وطلب حذف البيانات ("الحق في النسيان").

5. دراسات حالة: اختراقات واقعية ودروس مستفادة

تعرضت عدة مؤسسات كبرى لهجمات كشفت عن ثغرات حرجة:

- أرشيف الإنترنت (أكتوبر 2024) :تعرض لاختراق بيانات وهجوم DDoS أدى لتسريب 31 مليون حساب .الدرس :لا توجد منظمة محصنة، والتواصل الشفاف مع المستخدمين أثناء الأزمة ضروري.
- المكتبة البريطانية (أكتوبر 2023) :هجوم ببرامج فدية (Rhysida) أدى لتسريب 600 جيجابايت من البيانات وتكلفة تعافي بلغت 6-7 مليون جنيه إسترليني .الدرس :غياب المصادقة متعددة العوامل (MFA) كان ثغرة قاتلة، والأنظمة القديمة تزيد من تعقيد التعافي.
- مكتبات تورنتو وسياتل :(2023-2024) هجمات برامج فدية تسببت في إغلاق الخدمات الرقمية والأنظمة الداخلية لعدة أشهر.

6. تأثير التقنيات الناشئة: سيف ذو حدين

تمثل التقنيات الحديثة فرصاً لتحسين الخدمة ولكنها تفرض مخاطر أمنية جديدة:

التقنية	الفوائد	المخاطر
الذكاء الاصطناعي(AI)	توصيات مخصصة، تحسين استرجاع المعلومات، وفهرسة آلية.	التحيز الخوارزمي، الافتقار للشفافية، والحاجة لمجموعات بيانات ضخمة تزيد من احتمالية الاختراق.
إنترنت الأشياء (IoT)	مراقبة الظروف البيئية وإدارة المساحات المكانية.	زيادة "سطح الهجوم" بسبب ضعف الأمن في الأجهزة، وجمع بيانات حساسة عن الحركة والموقع.

الحوسبة السحابية	الوصول عن بُعد، القابلية للتوسع، وفعالية التكلفة.	مخاوف بشأن سيادة البيانات، والاعتماد على أمن الطرف الثالث (المزود السحابي).
سلسلة الكتل (Blockchain)	نزاهة البيانات، الحفظ الرقمي الآمن، واللامركزية.	عدم كفاية الخصوصية في السجلات العامة، والتعارض مع "الحق في النسيان" بسبب عدم قابليتها للتعديل.
تحليلات البيانات الضخمة	رؤى لتحسين الخدمات على مستوى كلي.	مخاطر إعادة تحديد الهوية (Re-identification) للمستخدمين من البيانات المجهولة، واستهداف المستودعات الضخمة للبيانات.

الخاتمة

تواجه المكتبات الرقمية تحدياً وجودياً في حماية خصوصية مستخدميها في ظل تصاعد التهديدات السيبرانية وتطور التقنيات. إن الاستثمار في التدابير الأمنية الاستباقية، والالتزام باللوائح القانونية، وتثقيف الموظفين والمستخدمين هي خطوات لا غنى عنها لضمان بقاء المكتبات الرقمية بيئات آمنة وموثوقة لتبادل المعرفة.