Entrepreneurship Journal for Finance and Business (EJFB)
2026, VOL. 07, NO. special, 75-87, E-ISSN: 2709-4251, P-ISSN: 2708-8790
DOI: https://doi.org/10.56967/ejfb2026920

Privacy digital data protection for university student in the smart universities environment

Anhar K. Mohammed*
Computer, Mosul University, Duhok, Iraq

Article information:
Published: 25–08– 2026

Corresponding author:
Anhar K. Mohammed
Rivers2013@yahoo.com

This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract:

The rapid shift towards artificial intelligence and its adoption in educational institutions to manage their educational and administrative affairs has produced large amounts of digital data.

The research aims to design an integrated governance framework to protect the privacy of student data, making the commitment to protection a competitive advantage not a functional burden.

The research used a comparative analytical approach to analyze institutional reports and documents. Among its findings was that the absence of governance in a smart university transforms data from a strategic asset into a source of risk that threatens the university's reputation.

This research presents a model based on three main dimensions P3: political, people, and Platform. This model is applicable to universities that rely on artificial intelligence, unlike previous studies that focused on these dimensions separately to address the problem of student data protection. The shortcoming of those studies lies in the absence of a clear model for the interaction of these three dimensions.

Keywords: Digital Data Protection, Artificial Intelligent, Smart Universities, Data Governance, University Entrepreneurship.

Conclusions:

The most important conclusion is the study's contribution to proposing a clear P3 model for data governance, which encompasses three dimensions simultaneously: policies, people, and platform.

This model achieves a balance between innovation and protection, fostering a competitive advantage. Also, storing student data in a unified university cloud to ensure digital sovereignty, and establishing a data ethics committee under the university presidency to review artificial intelligence projects before their launch.

حماية خصوصية البيانات الرقمية للطالب الجامعي في بيئة الجامعات الذكية

انهار خيرالدين محمد*
الحاسبات، جامعة الموصل، دهوك، العراق

معلومات البحث:
• تاريخ النشر: 2026 –08– 25

المؤلف المراسل:
انهار خيرالدين محمد
Riverskm2013@yahoo.com

هذا العمل مرخص بموجب المشاع الابداعي نسب المصنف 4.0 دولي (CC BY 4.0)

المستخلص

أدى التحول السريع نحو الذكاء الاصطناعي واعتماده في المؤسسات التعليمية لإدارة شؤونها التعليمية والإدارية إلى إنتاج كميات كبيرة من البيانات الرقمية.

يهدف البحث إلى تصميم إطار حوكمة متكامل لحماية خصوصية بيانات الطلاب، مما يجعل الالتزام بالحماية ميزة تنافسية وليس عبئًا وظيفيًا.

اعتمد البحث المنهج التحليلي المقارن لتحليل تقارير المؤسسات والوثائق. ومن أبرز الاستنتاجات التي توصل إليها أن غياب الحوكمة في الجامعة الذكية يؤدي إلى تحول البيانات من أصل استراتيجي إلى مصدر مخاطر يهدد سمعة الجامعة.

يقدم هذا البحث نموذجًا قائمًا على ثلاثة أبعاد رئيسية P3: السياسة، والبشرية، والمنصة. هذا النموذج قابل للتطبيق على الجامعات التي تعتمد على الذكاء الاصطناعي، على عكس الدراسات السابقة التي ركزت على هذه الأبعاد بشكل منفصل لمعالجة مشكلة حماية بيانات الطلاب. ويكمن قصور تلك الدراسات في غياب نموذج واضح لتفاعل هذه الأبعاد الثلاثة.

الكلمات المفتاحية: خصوصية البيانات الرقمية، الذكاء الاصطناعي، الجامعات الذكية، حوكمة البيانات، ريادة الأعمال الجامعي.

المقدمة:

يشهد العالم في قطاع التعليم العالي تحولاً رقمياً كبيراً ومتسارعاً في مجالات الذكاء الاصطناعي، مما يستوجب تحولاً جذرياً في طبيعة التعليم العالي فظهر ما يسمى بالجامعات الذكية التي تعتمد في عملها الأكاديمي والإداري على الأنظمة الرقمية.

هذه التحولات الرقمية زادت من حجم "البيانات" المجمعة وعظمت مسؤولية الجامعة في صيانة و "حماية البيانات "، وأصبح قرار الطالب بالالتحاق بالجامعة والاستمرار بها مبني على الثقة في الحفاظ على بياناته.

عالمياً بدأت الجهات التشريعية والمنظمات الدولية ومنها توصيات اليونسكو لأخلاقيات الذكاء الاصطناعي واللائحة الاوربية "لحماية البيانات" GDPR وارشادات منظمة التعاون الاقتصادي OECD في التعامل مع حماية خصوصية البيانات كحق اساسي وكمسؤولية شاملة تتقاطع فيها الادارة الأكاديمية، القانونية، والتقنية.

لم تعد الجامعات تقاس بجودة مختبراتها ومحاضراتها فقط بل بمدى امكاناتها على التنبؤ بمسار الطالب الأكاديمي وفهم احتياجاته، واتخاذ قرارات ادارية مبنية على الأدلة.

رغم الاستثمار الكبير للبنية التحتية الرقمية للجامعات في المنطقة العربية لايزال الإطار الحوكمي لاستخدام البيانات بشكل منظم غير مكتمل، فمعظم الجامعات التي تتبنى ادوات وانظمة الذكاء الاصطناعي بسرعة دون موازاة ذلك بأدوار محددة وسياسات واضحة وآليات تضمن عدم تحول "البيانات" إلى مصدر مخاطرة.

قسمت الدراسة الى خمسة محاور، تناول المحور الأول منهجية البحث، وتضمن المحور الثاني الدراسات السابقة بينما تضمن المحور الثالث الجانب النظري، في حين خصص المحور الرابع نموذج الحوكمة المقترح، وأخيراً خصص المحور الخامس لاستعراض اهم النتائج والتوصيات.

المحور الأول: منهجية البحث

1. مشكلة البحث:

أصبحت البيانات الرقمية الخاصة بالطالب الجامعي وقوداً لتشغيل أنظمة الذكاء الاصطناعي الخاصة في الجامعات لكن كل معلومة تُجمع هي مسؤولية مثلاً: تخصيص التعلم، أتمتة القرارات الإدارية.. الخ

إن متوسط كلفة اختراق البيانات بلغ 4.45 مليون دولار للحادثة الواحدة حسب تقرير IBM 2023 وأن الأعلى تكلفة هي القطاعات التعليمية بسبب طول الفترة التي يتم فيها اكتشاف الاختراق التي تصل الى حوالي277 يوم ولا توجد حوكمة قانونية واخلاقية موحدة لحماية بيانات الطلبة رغم الاستثمار الحاصل في البنية "التحتية الرقمية"، وهذا مما يشكل تهديداً على استدامة التحول الرقمي.

وقد اجرت كلاً منIBM ومعهدPokémon بحثاً عالمياً جديداً كشفت فيه أن أنظمة الذكاء الاصطناعي غير الخاضعة للحوكمة هي الاكثر عرضةً للاختراق وهذا مما يتسبب عنه تكاليف مالية عالية عند حدوثه.

لذا فإن مشكلة الدراسة تنطلق من التساؤل الاتي: هل يمكن وضع إطار حوكمة واضح وملائم للسياق الجامعي يتم فيه التحكم بجمع ومعالجة واستخدام بيانات الطالب في بيئة الجامعات التي تعتمد على الذكاء الاصطناعي وبما ينسجم ومتطلبات الخصوصية ومنعاً لانتشار الذكاء الاصطناعي الظلي؟

أهمية البحث:

لم تعد ريادة الأعمال الجامعية مقتصرة على إنشاء شركات ناشئة، بل امتدت لتصبح ريادية في إدارتها وأصولها من خلال إعادة تصميم المؤسسة نفسها.

البيانات موثوقة الحوكمة تفتح فرصاً للشراكة والتمويل مع الصناعة وتسويق الجامعة كجهة موثوقة وآمنة.

أهداف البحث:

للدراسة عدة أهداف منها:

1. دراسة خصوصية البيانات الرقمية للطالب.
2. مراجعة ودراسة الأطر الدولية لاستخلاص الدروس التي يمكن الاستفادة منها.
3. بناء نموذج حوكمة P3 قابل للتطبيق.
4. تقديم توصيات لتقليل مخاطر الاختراق والتسريب في البيانات التعليمية الرقمية في بيئة الجامعات الذكية.

الفرضيات:

لتحقيق الاهداف البحثية والاجابة على التساؤل في المشكلة البحثية انطلقت الدراسة من الفرضية الاتية: (يمكن وضع إطار حوكمة واضح وملائم للسياق الجامعي يتم فيه التحكم بجمع ومعالجة واستخدام بيانات الطالب في بيئة الجامعات التي تعتمد على الذكاء الاصطناعي).

أسلوب البحث:

اعتمد البحث المنهج الوصفي في تقديم المفاهيم والجانب النظري من الدراسة، والمنهج التحليلي المقارن وتقارير الحوادث الأمنية الجامعية، واللائحة الاوربية لحماية "البيانات GDPR"، وتختلف هذه الدراسة عن الدراسات السابقة بأنها ركزت على الأبعاد الثلاثة معاً "السياسات" "الأفراد" "المنصة" لبناء الثقة المؤسسية ولضمان "حماية البيانات" الخاصة للطلاب ضمن نموذج متكامل.

المحور الثاني: الجانب النظري

أولاً: مراجعة الدراسات السابقة

1. دراسة Al-Mutairi, (2023)

استخدم الباحث المنهج الكمي على عينة مكونة من (450) عضو من اعضاء هيئة التدريس في خمس جامعات حكومية في السعودية. هدفت الدراسة إلى دراسة أثر الحوكمة التقنية على خصوصية البيانات الخاصة بالطلاب في هذه الجامعات الخمسة السعودية. واهم النتائج التي توصلت اليها الدراسة هي وجود ما نسبته 27% من الالتزام بالسياسات وهذا يفسر بغياب التدريب لأعضاء هيئة التدريس، وما نسبته 38% من التباين في مستوى الثقة الطلابية يفسر بعدم وجود سياسات منظمة وواضحة خاصة بالبيانات، وتختلف هذه الدراسة عن الدراسة الحالية بأنها ركزت على بعدي "السياسات" والبعد التقني" فقط ولم تتناول في دراستها على بُعد "الأفراد" كعامل مستقل في نموذج متكامل.

2. دراسة الشهواني، محمد، والقحطاني، علي، (2022).

استخدم الباحثان المنهج الوصفي المسحي على عينة مكونة من 120 موظفاً تقنياً في ثمانية من الجامعات السعودية اهم اهداف الدراسة هي تحليل مدى مستوى الوعي الأمني المتواجد لدى موظفي تقنية المعلومات في هذه الجامعات الثمانية السعودية وبإمكانياتهم في منع اختراقات "البيانات". واهم النتائج هي أن 62% من المشاركين لم يتدربوا على الهندسة الاجتماعية، وأن عدد الحوادث الأمنية لا يتناسب مع الوعي الأمني. وتتفق هذه النتيجة مع البحث من حيث التأكيد على أهمية بُعد "الأفراد" في نموذج 3P.

3. Krause et al. (2021)

اجرى الباحثون في الجامعات الأسترالية للأعوام بين 2017-2020تحليل لـ 12 حالة من اختراق "للبيانات" وجدوا أن 74% من الحوادث سببها خطأ بشري وليس خلل تقني، منها ادخال كلمات مرور ضعيفة أو إرسال بيانات غير صحيحة.

وأهم التوصيات هي ضرورة اتخاذ قرار بضرورة اجراء تدريب إجباري للجميع وبناء ثقافة لدى العاملين بالإبلاغ عن الأخطاء. وهذا يدعم البحث بشكل مباشر بُعد "الأفراد"، ويبرر لماذا لا تكفي الحلول التقنية وحدها.

إن الدراسات السابقة ركزت على أبعاد منفصلة لمشكلة حماية بيانات الطلاب في عصر الذكاء الاصطناعي. وهنا تتضح الفجوة البحثية في غياب نموذجاً واضحاً لتفاعل الأبعاد الثلاثة معاً "السياسات" "الأفراد" "المنصة" لبناء الثقة المؤسسية ولضمان حماية البيانات الخاصة بالطلاب.

وهنا تكمن مساهمة الدراسة الحالية في اقتراح نموذج واضح وشامل للأبعاد الثلاثة قابل للتطبيق في الجامعات التي تستخدم الذكاء الاصطناعي.

المحور الثالث: الجانب النظري

أولاً: الجامعات الذكية

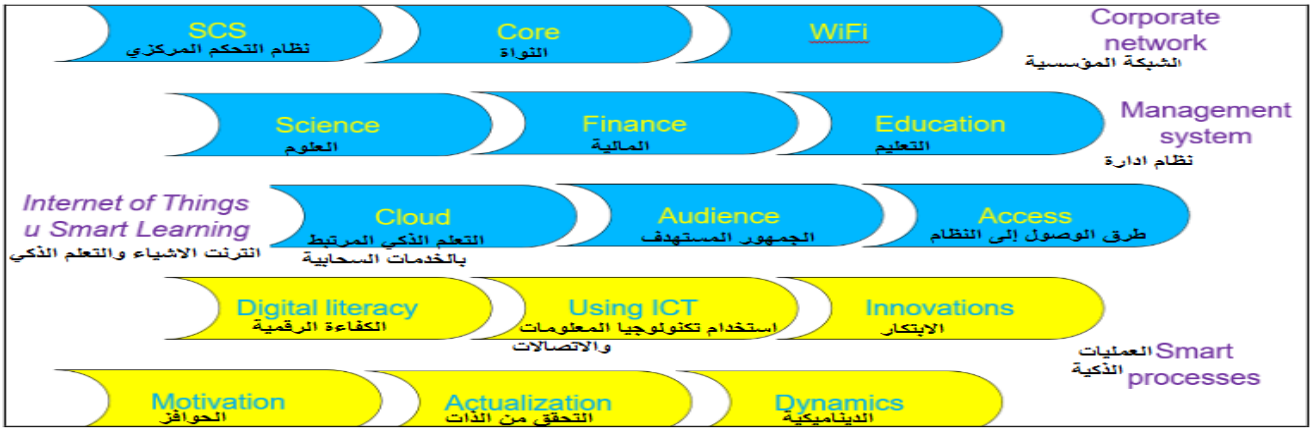
1.1.3: مفهوم الجامعات الذكية

أحد أبرز التوجهات الحديثة هو ما يعرف بالجامعات الذكية وعرف (الشايع،2021: 45) الجامعة الذكية "مؤسسة تعليمية تستخدم التكنولوجيا والابتكار لتعزيز تجربة التعلم وتحسين البيئة الاكاديمية والإدارية".

وعرفتها كلاً من (مساهل، 2024: 366) هي "جامعة تمتلك بنية تحتية مادية وتقنية وتدمج الابتكارات التكنولوجية والإنترنت لتوفر نوعية جديدة من العمليات التعليمية والعلمية ولتدعم متطلبات التعليم الذكي".

بينما عرفها كلاً من (عبد الله وطاهر،2025: 208) "جامعة ذات كفاءة وفعالية عالية تقدم تعليم مرن ومتطور باستخدام تقنيات المعلومات والاتصالات بهدف بناء انسان قادر على العيش في مجتمع المعرفة وتحويله من مستهلك الى منتج للمعرفة من خلال بيئة تنظيمية ذكية ومحتوى وبرامج تعليمية ذكية وابنية ذكية وتمويل ذكي وقيادة وإدارة ذكية"

قدم Vadym Kaptu خطة لنظام تعليمي ذكي شامل ومتكامل وكما موضح في الشكل (1)



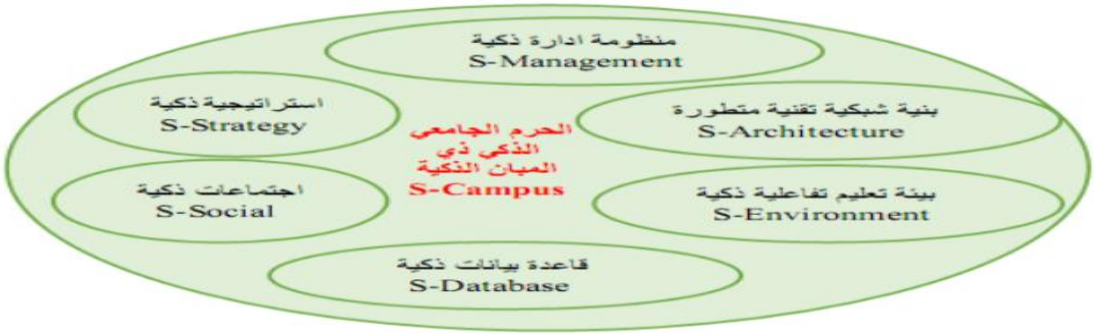
الشكل (1): خطة لنظام تعليمي ذكي شامل ومتكامل
المصدر:(Vadym Kaptur,2019: 90)

تعد جامعة حمدان بن حمد الذكية تحت اشراف سمو الشيخ حمدان بن حمد آل مكتوم والتي اقيمت في دبي اول جامعة ذكية عربية على مستوى الشرق الاوسط، ورسالة الجامعة هي تقديم طرق مبتكرة ومميزة في التعلم ونشر المعرفة والعلم باستخدام التطبيقات المبتكرة في التعليم والبحث العلمي (ممدوح، 2023: 57)

2.1.3: مكونات الجامعة الذكية

اهم مكونات الجامعة الذكية هي:

1. **الأنظمة الذكية:** هي عبارة عن" ارتباط بين مجموعة من الشبكات وذلك للتفاعل وزيادة الارتباط بين العناصر الإلكترونية المتواجدة داخل المبنى الجامعي منها (شبكة 5G،Wi-Fi 6)، خوادم سحابية (Cloud Computing)، واجهزة انترنت الاشياء
2. **الحرم الجامعي الذكي:** ويشمل المباني الجامعية في البنية التحتية لأنظمتها والتقنية الذكية، وكما موضح في الشكل (2)



الشكل (2): الحرم الجامعي الذكي
المصدر:(Mauro etal , 2014: 1003-1011)

3. **الادارة الذكية:** تشمل برامج إدارة ذكية على مستوى المؤسسات العالمية التعليمية لأنظمة التعليم الطلابي.

3.1.3: متطلبات التحول نحو الجامعة الذكية

أبرز متطلبات التحول نحو الجامعة الذكية (المسوري والكعدني،2024: **143-168**) (سلطان،2020: 310) هي:

1. **أشخاص أذكياء (كوادر بشرية ذكية):** هم الاشخاص الذين لهم القدرة على ايجاد حلول ذكية للمشكلات التعليمية والادارية سواء كانوا (أعضاء الهيئات التدريسية، والعاملين، والقادة وهم من أكثر العوامل للتحول نحو نموذج الجامعات الذكية)

واهم "الموارد البشرية" للجامعة الذكية موضحة في الشكل (3)



الشكل (3): "الموارد البشرية للجامعة الذكية
المصدر: من اعداد الباحثة

2. **بيئة تعليم ذكية:** تتطلب تهيئة بنية تحتية تقنية متطورة لمواكبة التطور الحاصل في جامعات العالم.
ويعتمد في تصميمها على مجموعة من التخصصات المختلفة منها الذكاء الاصطناعي، شبكات الاستشعار، الوسائط المتعددة، وشبكات الاستشعار.
3. **قيادة إدارية رقمية:** يرتبط نجاح الجامعات الذكية بقيادة وادارة بيئات كفؤة وفاعلة تنسق جهود جميع افرادها في تحويل جميع العمليات الادارية الورقية الى عمليات ادارية الكترونية باستخدام التقنيات الرقمية المختلفة.
4. **خطط استراتيجية واضحة وشبكة معرفة ذكية:** وتعني وضع خطط استراتيجية للجامعة. تمكن الجامعة من مواجهة مختلف التحديات التي تواجه الجامعة.
5. **أبنية ذكية:** تضم بنية تحتية تقنية ومادية مجهزه بنظام اداري وتكنولوجي داخل الحرم الجامعي وتصمم المباني بطريقة ذكية معقدة تقنياً ومجهزه بنظام ادارة ذكي يستخدم اجهزة رقابة واستشعار في جميع المباني وايضاً وجود قاعات ومعامل ومكتبات ذكية، فضلاً عن الترشيد في الاستهلاك للطاقة والمياه، توفير شبكات الأنترنت، وضمان سلامة الافراد وحمايتهم.

والشكل (4) يوضح متطلبات الجامعة الذكية



الشكل (4): متطلبات الجامعة الذكية
المصدر:(اللاوي وسيرات،2024: 30)

4.1.3: خصائص الجامعة الذكية

يوجد للجامعة الذكية مجموعة من الخصائص ومن أبرز هذه الخصائص (عبدلي،2025: 10) (بن منصور،2025: 150-151):

1. **المستودعات الجامعية الرقمية الذكية**: تشمل الإنتاج العلمي في ظل تقنيات الذكاء الاصطناعي.
2. **التعليم المتنقل:** هو من أهم وأبرز خصائص الجامعة الذكية، ومن خلاله يمكن الوصول إلى المحتوى العلمي في أي وقت وفي أي مكان.
3. **التعليم الفردي:** إعطاء خصوصية شخصية للتعليم لكل فرد، كما تهدف إلى تصميم بطاقات التعليم الفردي.
4. **إمكانية الوصول:** وهي من أهم خصائص الجامعة الذكية، حيث تهدف إلى تسهيل عملية الوصول إلى الخدمات التعليمية عن طريق الإنترنت.
5. **الفعالية التقنية:** يتم استخدام التقنيات السحابية، والافتراضية لتوفر صلاحيات البنية التحتية لتقنية المعلومات في الجامعة الذكية.
6. **الانفتاح:** يقصد أن يكون هناك مجموعة من المستودعات المفتوحة والتي تتكون من مجموعة كبيرة من المصادر والمواد التعليمية.

وتشكيل دورات التعلم الإلكتروني والتدريب للطالب في كافة التخصصات، للوصول بكل حرية إلى الأبحاث والمصادر.

ثانياً: خصوصية البيانات الرقمية للطالب: المفهوم والأبعاد القانونية والأخلاقية

1.2.3: خصوصية البيانات الرقمية

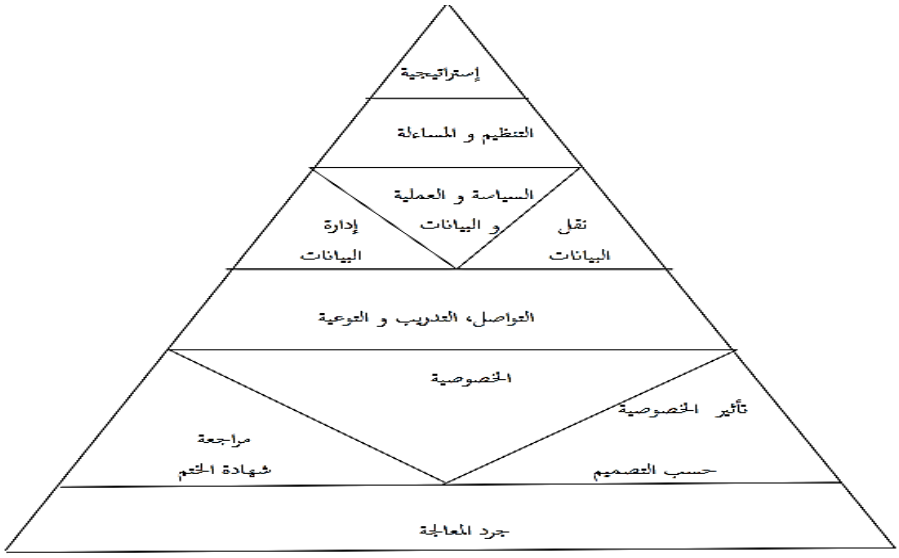
تثار الكثير من المخاوف بشأن انتهاك خصوصية الافراد من قبل تطبيقات الذكاء الاصطناعي التي تعتمد على جمع البيانات ومعالجتها والتي تعد من أهم الحقوق المتعلقة بحق الفرد في حماية حياته الخاصة ومنع الوصول اليها واستخدامها من دون الموافقة من الشخص المعني.

حماية البيانات الشخصية هي مسؤولية مشتركة بين الأفراد والمؤسسات الحكومية، واوائل الدول التي اهتمت بحماية البيانات الشخصية هي بريطانيا حيث اصدرت في عام 1998م قانون حماية البيانات الشخصية وهي "البيانات المتعلقة بالشخص الحي الذي يمكن تعريفه بها أو بضمها لمعلومات

اخرى أو بحوزة المسؤول عن معالجة البيانات، أو من المحتمل أن تكون في حوزته"

وعرفتها اللائحة للاتحاد الاوربي بأنها" أي معلومات تتعلق بشخص طبيعي أو يمكن التعرف عليه بشكل مباشر أو غير مباشر وخصوصاً المعرف به مثل الاسم/بيانات الموقع/رقم تعريف/معرف عبر الانترنت/او أكثر العوامل المعرفة للهوية الجسدية/الفسيولوجية، العقلية / الوراثية/ الاقتصادية/الثقافية/ الاجتماعية لذلك الشخص".

واهم إجراءات GDPR موضحة في الشكل (5)



الشكل (5): إجراءات اللائحة العامة لحماية البيانات

المصدر(Deloitte. 2018: 11)

بينما عرفها المشرع الاردني لقانون "البيانات" الحساسة "هي البيانات التي تشكل معالجتها مخاطر أو تمييزاً بالنسبة إلى حماية الحياة الخاصة للشخص، كأن تبين الأصل العرقي، أو الآراء والاتجاهات السياسية والمعتقدات الدينية، أو أي بيانات تتعلق بحالته الصحية أو الجسدية أو العقلية أو الاقتصادية، أو انتماءاته الحزبية أو سجله الاجرامي"(العاني ويوسف،2026: 492)

فالخصوصية هي احدى حقوق الانسان وتعتمد اساساً على البيئة وعليه تختلف تعاريف الخصوصية من بيئة إلى اخرى وتعرف الخصوصية " بقدرة الشخص بالتحكم ببياناته وعدم قدرة الغير على الوصول لتلك المعلومات دون اذنه، وان هذا الحق ملتصق بالشخص الطبيعي لكونه حقاً من حقوق الانسان إلا أنه يجب أن يضمن القانون حقوق الشخص كونه له سمعه واسرار " (قدوري،2024 :252-253).

أول مرة اثيرت فكرة الخصوصية على يد المؤلف (Alan Weston) في كتابه الخصوصية والحرية لعام 1967م والذي عرفها ("حق الأفراد في تحديد متى وكيف والى اي مدى تصل المعلومات عنهم للآخرين") وعلى يد المؤلف الامريكي (Miller) عام 1971م ضمن كتاب: الاعتداء على الخصوصية وعرفها (Miller) ("قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم).

وطرح في العصر الرقمي مفهوم الحق في الخصوصية عام 2013م وبشكل مباشر عندما قام (ادوارد سنودن) وهو موظف في الاستخبارات الامريكية بالتجسس على 35 من رؤساء وزعماء العالم حيث تم نشر تقريراً مفصلاً من قبل صحيفة الغارديان البريطانية تكشف فيه عن برنامج (PRISM) الذ تم استخدامه من قبل الشركات الكبرى YouTube Google وFacebook وبالتعاون مع وكالة الأمن القومي الأمريكي حيث أن البرنامج يوفر مراقبة واسعة على المعلومات المخزنة والاتصالات الخاصة بالأفراد فضلاً عن استهداف اي مشترك أو عميل مع الشركات.

ومن هنا بدأ الحديث عن الخصوصية الرقمية والمرتبطة بحماية بيانات الأفراد سواء اكانت في المستودع الرقمي بالشركات الأم والخاصة بمواقع التواصل الاجتماعي أو المستودع الرقمي الحكومي.

عرف الخصوصية الرقمية (الدرواس،2024،189) بانها" الحق في التحكم في جمع واستخدام وكشف المعلومات الشخصية في البيئة الرقمية، ويشمل الحق في حماية البيانات من الوصول غير المصرح أو الاستخدام غير المشروع".

وعرفها كلا من (الشباطات والوحشات،2025: 71) هو" حق الشخص في حماية بياناته ومعلوماته واتصالاته ومراسلاته في الفضاء الالكتروني وعلى أجهزته الرقمية وحقه في التحكم في جمعها وحفظها ومعالجتها واستخدامها وفقاً للقانون وبما يتفق مع الغرض الذي جمعت من اجله".

بينما عرفتها (الحربي،2026: 14) " حماية خصوصية الفرد من تطبيقات الذكاء الاصطناعي".

فالحق في الخصوصية الرقمية هو حق ثابت ومحدد وتنظمه الدول المتقدمة، والمؤسسات الحكومية التي تتعامل مع بيانات الاشخاص الالتزام بمعايير صارمة لحماية خصوصية

البيانات للحفاظ على ثقة الافراد وتجنب التبعات القانونية الناجمة عن اختراقات البيانات.

تُعد بيانات الطلاب في البيئة الجامعية سواء اكانت اكاديمية أو مالية أو صحية فضلاً عن بيانات البيو مترية مثل التعرف على الوجه او بصمات الاصابع عند استخدام الانظمة الرقمية هدفاً للهجمات الإلكترونية، حيث تشهد الجامعات والمدارس اختراقات أمنية متكررة تشمل هذه البيانات سجلات الحضور، الدرجات، والموقع، ويجب على الجامعات والمؤسسات التعليمية استخدامها بشكل آمن ومسؤول، والالتزام بقوانين ولوائح "حماية البيانات" للحفاظ على خصوصية الطالب. وهذا التطور يتطلب ضوابط قانونية تلزم بها المؤسسات الجامعية لضمان عدم إساءة استخدامها وللحفاظ على الخصوصية وحمايتها وحماية الامن القومي (Hoofnagle, etal ,2019: 65-98).

2.2.3: الأبعاد القانونية

ان تحقيق تعليم رقمي فعّال ليس فقط بالاعتماد على التقنية، بل على منظومة أخلاقية متكاملة؛ فكلما ازدادت قدرة الجامعات على دمج المبادئ الاخلاقية في تجربتها التعليمية، زادت قدرت الجامعة على إعداد جيل قادر على مواجهة التحديات بثقة ومسؤولية من الخريجين ولذلك يُعد الالتزام بالأخلاقيات واجبًا أكاديميًا وأخلاقيًا أصيلًا في التعليم الرقمي

تخضع الجامعات الرقمية لمنظومة صارمة من اللوائح والتشريعات المحلية والدولية لضمان حماية قواعد البيانات وتجريم أي اختراق لها، وتشمل: (ابراهيم وجاسم،2025: 1-7) و (عزيز،2026:1-18) (الصغير،2026: 311-339) (Dharma & etal,2024: 1644-1656)

1. **التشريعات الدولية والوطنية :**تُلزم القوانين الحديثة المؤسسات بتطبيق معايير واضحة لجمع ومعالجة بيانات الطلبة.

وأبرز القوانين الدولية هي اللائحة العامة لحماية البيانات لعام 2016م والتي اصدرها الاتحاد الاوربي حيث فرضت التزامات صارمة على المنظمات لضمان حق الافراد في حالة الوصول الى بياناتهم.

اما أبرز القوانين في العراق هو قانون العقوبات العراقي رقم 111 لسنة 1969م الذي يجرم التعدي على المعلومات الشخصية، وقانون المعاملات الالكترونية رقم 78 لعام 2012م الذي ينظم العديد من جوانب "حماية البيانات" في البيئات الرقمية، كما تفرض القوانين العراقية على المؤسسات الحكومية ومنها الجامعات باتخاذ التدابير الامنية لحماية المعلومات في حالة تم استخدامها لأغراض غير قانونية لكن تبقى "البيانات الشخصية" عرضة للمخاطر في العراق مما يتطلب تحديث مستمر للقوانين في ظل التحول الرقمي المتسارعة

2. **حدود الاستخدام والجمع :**يتم "الحد الأدنى" في جمع البيانات الضرورية بالجامعات الذكية لأغراض أكاديمية محددة ومعلنة مسبقاً، مع عدم السماح باستخدامها تجارياً من دون موافقة صريحة.
3. **الالتزام بالشفافية :**الوضوح التام مع الطلبة والموظفين عن ماهية البيانات المُجمّعة وكيفية تحليلها (مثل السجلات الأكاديمية، والتقارير الصحية، والموقع الجغرافي) حيث يسمح للمستخدم الاطلاع على بياناته وفق سياسات محددة، وتعديلها، أو طلب حذفها.
4. **المسؤولية القانونية والجزائية :**تفرض القوانين عقوبات صارمة على الجهة التعليمية أو مسؤولي معالجة البيانات عند تسريب قواعد بيانات الطلبة بصورة غير مشروعة.
5. **التحيز والعدالة :**التأكد من أن أنظمة التقييم والقبول الإلكترونية وخوارزميات الذكاء الاصطناعي عادلة ولا يوجد أي تمييز او تحيز بين الطلبة.
6. **الموافقة المستنيرة :**الحصول على موافقه من الطالب لجمع أو استخدام بياناته في أنشطة البحث العلمي دون إجبار أو استغلال.

3.2.3: الأبعاد الأخلاقية

الاخلاقيات الرقمية هي "مجموعة المبادئ والقيم التي تهدف إلى توجيه استخدام التكنولوجيا الرقمية بطريقة تراعي احترام الحقوق الفردية والجماعية "

فقد اصبحت اليوم "التكنولوجيا الرقمية" تدخل في مختلف نواحي الحياة مما يتطلب توازناً بين حماية حقوق الانسان والابتكار وأبرز القيم التي تشكل جوهر الاخلاقيات الرقمية هي (بن صغير،2021: 208-227) (بن زكريا،2021: 208-227) (البوحنيه، 2025: 477-521):

1. **"حماية خصوصية البيانات":** تعتبر حماية البيانات من الامور البالغة الاهمية إذ يمكن أن يتعرض الاشخاص الى مخاطر الاستغلال او التسريب ومن بين أبرز القضايا هي فضيحة "كامبريدج أناليتيكيا" التي تم فيها استخدام ملايين من بيانات المستخدمين على الفيس بوك من دون الاخذ بموافقتهم لأغراض سياسية وهذا مما يؤكد على ضرورة حماية "البيانات الشخصية".
2. **الشفافية:** تشمل الشفافية في طريقة جمع البيانات ومعالجتها ويتوجب على المؤسسات توفير المعلومات الخاصة بسياسات الخصوصية وشروطها هذا يسهم في بناء الثقة لدى المستخدمين حول استخدام "التقنيات الرقمية".
3. **العدالة والمساواة:** تسعى الاخلاقيات الرقمية الى توفير ضمان وصول متساوي وعادل للتقنيات إلى جميع الفئات الاجتماعية خاصة في مجتمعات الدول النامية.
4. **المسؤولية الرقمية:** تتحمل المؤسسات المسؤولية عن جميع قراراتها المعتمدة على التقنيات الذكية.

ثالثاً: حوكمة البيانات

1.3.3: مفهوم حوكمة البيانات

اصبحت البيانات تمثل النفط الجديد والمحرك الاساسي للمنافسة في القطاعات المختلفة وخاصة قطاع التعليم العالي. فيجب أن يكون للبيانات في الجامعات الذكية لها أنظمة وقوانين تحكمها لأنها تنتقل من مكان إلى مكان آخر.

وتعتبر "حوكمة البيانات" الأساس لتنظيم البيانات داخل الجامعات، مما يضمن جودتها، ودقتها، والامتثال للمعايير القانونية.

وتبرز اهمية "حوكمة البيانات" في ظل سرعة التحولات الرقمية، حيث تساعد المؤسسات على ادارة البيانات بطريقة مسؤولة وتضمن استدامتها.

ويعود أصل مصطلح الحوكمة إلى كلمة اغريقية قديمة والتي توضح امكانيات صاحب السفينة في اداء مهمته بإدارة حكيمة والتي تعني "اسلوب ممارسة سلطات الادارة الرشيدة". (حكمت ،311، 2020).

وتعرفها كلاً من (بن عيدة وبحصوص) "الادارة الشاملة لتوافر البيانات، وسهولة الاستخدام، والنزاهة، والجودة، وأمن البيانات". (بن عيدة وبحصوص،2024: 155-190)

2.3.3: مبادئ حوكمة البيانات

اهم المبادئ الاساسية لحوكمة البيانات عند استخدام أنظمة الذكاء الاصطناعي هي (Camilleri,2023: 5) (Rene,2019,P.11) -(Kwon, J. ,2023: 1) :

1. **العدالة:** يتم اختيار البيانات دون تمييز سواء اكان تمييز فكري، عرقي، عنصري، الخ لغرض تحليلها بشكل موضوعي وعادل.
2. **الشفافية:** يتم بناء النماذج لأغراض التنبؤ وانظمة الذكاء الاصطناعي بدرجة من الوضوح والشفافية مع امكانية تتبع اتخاذ القرارات بشكل آلي التي قد تتسبب بأضرار مادية على صاحب البيانات.
3. **المسؤولية:** تقييم الآثار والمخاطر المحتملة من استخدام انظمة الذكاء الاصطناعي عند استخدامها بشكل غير مسؤول.
4. **الشمولية**: يجب ان تشمل عينة البيانات المراد تحليلها مختلف فئات المجتمع دون أي تحيز.
5. **الانسانية:** يجب ان يتم بناء انظمة الذكاء الاصطناعي وفق منهجية اخلاقية قائمة على القيم والحقوق الانسانية.
6. **الأمان:** يجب يتم استخدام انظمة الذكاء الاصطناعي بطريقة آمنة مع امكانية التحكم بها من دون الحاق أي ضرر.
7. **جودة البيانات:** يجب ان تكون البيانات صحيحة ودقيقة وموثوقة المصادر مع امكانية تحديثها بصورة مستمرة.
8. **حقوق اصحاب البيانات:** يجب أن يكون في سياسة حماية البيانات حقوق لصاحب البيانات الشخصية.

اما اهم عناصر حوكمة البيانات موضحة في الشكل (6)



الشكل (6): عناصر حوكمة البيانات
المصدر: من اعداد الباحثة

3.3.3: الحوكمة الرشيقة للبيانات

لتمكين المؤسسات من إدارة بياناتها بفعالية والتكيف في بيئة رقمية سريعة التطور قائمة على البيانات يتم الاعتماد على نهج حديث ورشيق لإدارة البيانات وتخفيف المخاطر وهو الحوكمة الرشيقة للبيانات التي تركز على المرونة والتعاون والتحسين التكراري (Pham bich Thuy & Pham Dao Tien,2025: 72)، ويجب أن تطبق بشكل رئيسي في الجامعات الذكية، لأن الجامعات الذكية طبيعة نظامها يستوجب تدفقاً فورياً للبيانات وهذا يتطلب إطلاق تطبيقها في "الجامعات الذكية".

إن "حوكمة البيانات التقليدية" هي "ممارسة الرقابة والسلطة (التخطيط-المراقبة-والتنفيذ)" (DMAA International,2017: 33).

اما حوكمة البيانات الرشيق فهي "نهج حديث يركز على المرونة والتعاون والتحسين التكراري من دون عوائق مركزية ادارية"(تفكجي،2026: 109-118).

والجدول (1) يوضح المقارنة بين الحوكمة الرشيقة للبيانات وحوكمة البيانات التقليدية

جدول (1): اوجه المقارنة بين الحوكمة الرشيقة للبيانات وحوكمة البيانات التقليدية

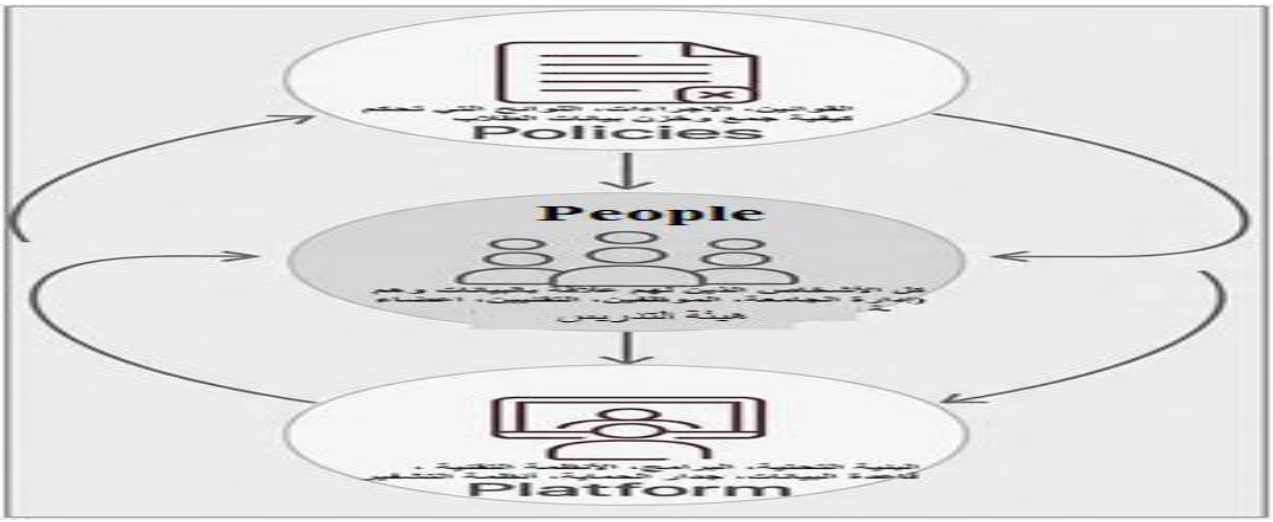
اوجه المقارنة	الحوكمة التقليدية	الحوكمة الرشيقة للبيانات
دعم القرارات الجامعية	**بطيئة:** طول دورة الموافقات الادارية، حيث يستغرق سحب البيانات واعداد التقارير لرئيس الجامعة او العميد وقت طويل	**فورياً:** تدفق البيانات إلى لوحة التحكم الذكية فوراً ويتم اتخاذ القرارات بصورة سريعة من قبل القيادات
"التعلم التكيفي"	**غير موجودة:** عدم قدرتها على تغذية البيانات بصورة فورية	**ممكنة:** توفر البيانات آلياً وبشكل مستمر
"الحماية وخصوصية البيانات"	**رقابية يدوية:** تعتمد على العنصر البشري في مراجعة المستندات للتأكد من عدم تسريب البيانات الحساسة او الدرجات	**ديناميكية ومؤتمتة:** يتم تطبيق سياسات الحجب والامن برمجياً وتمنح الصلاحيات بشكل مؤقت وتلقائي
ادارة الحرم الجامعي	**محدودة الاستفادة:** ليس لها القدرة على التعامل مع بيانات المستشعرات الخاصة بالحرم الجامعي	مباشرة ومستدامة تحكمها IOT لتسهيل العمليات اللوجستية التي تتم داخل الحرم الجامعي، وترشيد استهلاك الطاقة
"إدارة التغيرات الحاصلة واللوائح"	**جامدة:** تحتاج الجامعة إلى وقت طويل لإجراء التعديل على سياسات البيانات لتواكب التقنيات الجديدة	تكرارية ومرنة ومواكبة للتطور
"التعامل مع البيانات"	**انظمة مغلقة ومنعزلة:** يتم الاحتفاظ بالبيانات بأنظمة مغلقة فمثلاً عمادة الكلية تحتفظ ببيانات (القبول، المكتبات، المالية الطالب من جميع النواحي. الخ ومن الصعوبة ربطها معا الا بعد الحصول على طلب رسمي ومعقد	**مدمجة** تربط "بيانات الطالب" بمنصة مرنة، هذه المنصة تسمح برؤية ملف

المصدر: من اعداد الباحثة

المحور الرابع: النموذج المقترح

1.4 مكونات النموذج المقترح

النموذج المقترح 3Pيتكون من ثلاث طبقات (السياسة-الأفراد-المنصة) يتم عملها ضمن حلقة مغلقة فعند حصول ضعف في طبقة واحدة تنتهي فاعلية الطبقتين الأخيرتين والشكل (7) يوضح الطبقات الثلاثة



الشكل (7): نموذج 3P
المصدر: من اعداد الباحثة

1. السياسات
P1: Policies

تحدد فيها كيفية استخدام الأشخاص للمنصة حيث أن الأفراد يشتغلون على المنصة ويطبقون السياسات.

هذه الطبقة تضع قواعد قبل البدء بالتشغيل وتحتوي على طبقتين:

- **الطبقة الأولى:** خاصة بالطلاب تعرض اجبارياً عند اول تسجيل للطالب ولا يمكن تجاوزها.

فبدل موافقة واحدة عند التسجيل يحصل الطالب على لوحة تحكمه بأمرين اما:

- **امر موافق:** الموافقة على استخدام بياناته لأغراض بحثية او تسويقية أو تنبؤيه...الخ
- **امر لا أوافق:** اي رفض الطالب على مشاركة بياناته مع شركاء ولأي غرض كان.

- **الطبقة الثانية:** هي وثيقة قانونية مفصلة.

2. الأفراد

P2: People

كل الاشخاص الذين لهم علاقة بالبيانات وهم (إدارة الجامعة، الموظفين، التقنيين، اعضاء هيئة التدريس)

الهدف منها هو كي يستطيع كل شخص أن يفهم ماهي مسؤولياته، واجراء التدريبات المستمرة لمواكبة التقنيات المتجددة.

3. المنصة

P3: Perform

هي الأنظمة التقنية، "البرامج"، "البنية التحتية"، "جدار الحماية"، "انظمة التشفير"، "قاعدة البيانات" وقد تم توضيحها في الشكل (7).

الاسهم الدائرية في الشكل (7) توضح أن الثلاثة(السياسة-الأفراد-المنصة) لا يشتغلون الواحد بمعزل عن الآخر حيث أن:

- السياسات(P1: Policies) تحدد وتوضح كيفية استخدام الأفراد للمنصة.
- الأفراد(P2: People) هم الافراد الذين يشتغلون على المنصة ويطبقون السياسات المفروضة والمحددة لهم.
- المنصة(P3: Platform) : هي التي يتم فيها فرض القيود على الأفراد لحماية بياناتهم وتنفيذ السياسات.

أي جزء من هذه الأجزاء الثلاثة يظهر فيها ضعف السلسلة كلها تنهار وعليه هذا النموذج يجب أن يتم فيه تقوية السياسات وتدريب الأفراد عليها وتأمين المنصة مع بعض.

2.4: المناقشة

المخاطر في بيئة الجامعات الذكية لها آليات محددة ولا تحدث بشكل عشوائي وغالباً ما يعود اسبابها إلى غياب الحوكمة واهم مخاطر "الجامعات الذكية" هي:

1. التسرب السيبراني

يحدث عندما توجد ثغرة في قاعدة البيانات المركزية للجامعة أو نظام إدارة التعلم أو الوصول الغير مصرح للبيانات داخل الجامعة أو الاحتيال والتصيد أو ضعف في إدارة كلمات المرور مما يتسبب في توقف أنظمة الامتحانات وأفضل مثال هو ما حدث لجامعة مانشستر عام 2023م حيث تم توقيف بحوث كانت ممولة بأموال طائلة لمدة ثلاثة أشهر.

2. المخاطر الناتجة عن تنفيذ خوارزميات الذكاء الاصطناعي

اهم اسباب حدوثها هو غياب فريق ذو تخصصات مختلفة يقوم بمراجعة مخرجات نموذج الذكاء الاصطناعي فضلاً عن القرارات غير المنصفة في التخصص المالي أو قرارات الانذار المبكر، والقرارات التي تخص التوصيات الاكاديمية، وهذا مما يعرض الجامعة إلى العديد من الدعاوى القضائية وهذا مما يضر بسمعة الجامعة الأخلاقية.

3. المخاطر التي تخص بفقدان السيادة

اجراءات الاختبارات لمزود الخدمة السحابية من دون مراجعة الشروط المتعلقة بالسيادة والاختصاص القضائي.

4. المخاطر التي تسببها الاستخدامات الغير معلنة

يتم مشاركة بيانات الطلاب مع جهة تجارية أو جهة غير مسموح لها باستخدام "البيانات" لأغراض مختلفة من دون اخذ موافقة قانونية وصريحة واسبابها عدم فصل بيانات التشغيل عن بيانات البحث أو.. الخ وهذا مما يتسبب في عزوف الطالب عن استخدام المنصات الرسمية وبالتالي يتسبب في فشل مشروع التحول الرقمي.

اما النموذج المقترح يقسم الحوكمة إلى ثلاث طبقات عملها ضمن حلقة مغلقة فعند حصول ضعف في طبقة واحدة ينهي فاعلية الطبقتين الأخيرتين.

تقنياً النظام يقرأ الاعدادات ويعمل على غلق الوصول آلياً في حالة رفض الطالب مشاركة بياناته وأيضاً يتم تحديد مدة زمنية للاحتفاظ بكل نوع من " البيانات".

هناك جدول مهام يقوم بالحذف للبيانات تلقائياً من قاعدة البيانات من دون تدخل بشري، فضلاً عن وجود لجنة قانونية مستقلة تقوم بمراجعة أي مشروع يقوم باستخدام بيانات الطالب سواء لأغراض بحثية أو لأي غرض آخر.

العنصر البشري هو خط الدفاع الأول حيث يعين مسؤول حماية للبيانات وهو شخص غير تقني يقوم بمراجعة المشاريع قبل البدء بإطلاقها وتلقي الشكاوى المقدمة من الطالب واصدار التقارير السنوية وبشكل علني عن حوادث البيانات التي حصلت خلال السنة وتوضيح الاجراءات التي تم اتخاذها.

فتح قناة ابلاغ مجهولة الهوية وسياستها هي منع اتخاذ أي اجراءات تأديبية عن الاخطاء الغير متعمدة والتي يتم الابلاغ عنها فالموظف الذي يقوم بالتبليغ المبكر عن اخطائه يكافأ ولا يعاقب الهدف هو كشف الخطر عن الاخطاء الغير متعمدة قبل أن تتحول إلى خرق كبير.

يضاف التشفير بأحدث طرق التشفير من البداية حيث يتم تحويل "البيانات" الصريحة إلى "بيانات" مشفرة يكون الوصول إليها مغلق افتراضياً وأي جمع للبيانات يتطلب الحصول على موافقة لجنة وهناك سجلات تدقيق تسجل فيها أي عملية عرض أو تعديل يتم اجراؤه على بيانات الطالب حيث يسجل فيها من اي جهاز تم اجراؤها، ومتى، ولماذا وتخزن في مكان خارجي لا يستطيع أي شخص حتى مسؤول النظام حذفه.

المراقبة المستمرة لأي عملية اختراق أو تصيد، وعند اكتشاف وصول غير صحيح أو غير طبيعي يرسل النظام تنبيه تلقائي لمسؤول الخصوصية.

عند طلب الحذف من الطالب تنفذ العملية بصورة آلية بعد 72ساعة ويتم بعدها ارسال اشعار للطالب مع رقم تتبع واي محاولة من موظف أو تدريسي للوصول الى بيانات طالب

معين ليس ضمن صلاحيته أو مسؤوليته يسجل هذا الحدث ويرسل بشكل فوري على شكل تنبيه.
واخيراً ...
الجامعات التي استثمرت في حوكمة واضحة قلّلت حوادث التسرب وفتحت باب الشراكات البحثية مع مؤسسات حساسة للخصوصية.

المحور الخامس: الاستنتاجات والتوصيات

اولاً: الاستنتاجات

1. "حماية خصوصية البيانات" والحفاظ عليها شرط ضروري وأساسي لنجاح الجامعات الذكية واستدامتها .
2. غياب حوكمة البيانات قد يؤدي إلى مخاطر مؤسسية تهدد سمعة الجامعة.
3. يحقق نموذج 3Pتوازناً بين الابتكار والحماية ويخلق ميزة تنافسية.

ثانياً: التوصيات

1. إنشاء وحدة في كل كلية هي وحدة حوكمة بيانات تكون تابعة لرئاسة الجامعة بصورة مباشرة ومستقلة.
2. تصميم لوحة تحكم خاصة بالطالب تمنح الطالب خصوصية وحرية التحكم ببياناته .
3. انشاء سحابة جامعية لاستثمارها في التخزين المركزي وطنية لضمان السيادة الرقمية .
4. استخدام مؤشرات ريادية لقياس العائد من الامتثال .
5. إنشاء لجنة أخلاقيات البيانات لمراجعة مشاريع الذكاء الاصطناعي في الجامعات الذكية قبل إطلاقها.
6. اعتماد الحوكمة الرشيقة للبيانات في بيئة الجامعات الذكية بدلاً عن حوكمة البيانات التقليدية.

تضارب المصالح:

تعلن الباحثة أنه ليس لديها تضارب في المصالح.

موارد التمويل:

لم يتم تلقي اي دعم مالي.

شكر وتقدير:

لا أحد.

References:

1. Al-Aidarous Nazeeha Mohammed Ali ،2024 ،Enhancing Awareness of Digital Privacy in the Social Networks Era an Empirical Study on Students of the Faculty of Computers and Information Technology at Hadhramout University, Al-RAYAN Journal, vol.7(13), P189.
2. Al-Ani, Mohammed Shalal, Fatma Yaqub Yousif, 2026, The Legal Nature of the Crime of Electronic Hacking That Harms State Security a Comparative Study, Journal of Legal Sciences,492.
3. ABdellaoui radja, sirat samia,2024, Requirements and Challenges of the Transition Towards the Smart University in Algerian Universities with Presentation of Successful Experiences, Electronic Business & Digital Economics Journal, P.30
4. Abdelli, Ahmed,2025 "Smart University Digital Repositories as a Tool for Marketing Scientific Production in Light of Artificial Intelligence Technologies: Requirements for Transitioning to Generation 4.0 University." *Proceedings of the Scientific Symposium/Laboratory of Da'wah and Communication Studies*, Faculty of Arts and Islamic Civilization, Emir Abdelkader University of Islamic Sciences, P.10.
5. Abdullah Abdul Majeed Shaima'a Salam, Taher Mohammed Al-Ahdal,2026, The extent to which Yemeni universities meet the requirements for transformation into smart universities, Sana'a University Journal of Human Sciences, Vol.4, No2, 208.
6. aben aida Fauziya, Bahsosee rekia, Data governance in higher education institutions, Al-Maghrebi Journal of Manuscripts vol20(1), pp155-190,
7. Albohnyah Abduliah,2025, Artificial Intelligence Ethics in Education: A Proposed Pedagogical Framework for Developing Teachers' Ethical Awareness in Saudi Arabia in Light of International and National Policy Documents, Education Journal, Vol.139, pp.477-521
8. Al-Masouri, Ibrahim Ahmed Saleh Hamid, Al-Kaadan Nasser Mohammad Ahmed,2024, Requirements for Transforming the Community College (Sana'a) into a Smart College from the Perspectives of Academic and Administrative Leaders, Sana'a University Journal of Human Science, vol.3, No4, PP143-168.
9. Al-Mutairi, A., et al. (2023). The reality of integrating educational technologies and

responsibility", John Wiley & Sons Ltd., Vol.41, No7, pp.1-5.

19. Deloitte NWE Privacy Services – Vision and Approach,) GDPR. 2018, p. 11

20. Dharma Setiawan Negara, Nunu Burhanuddin, Abu Sahman Nasim,Juni Irianti Sitinjak, Johannes Johny, 2(7):1644-1656

21. DMAA International,2017, DAMA-DMBOK: Data Management Body Of Knowledge,2nd, Technics Publishing, P.33

22. EEE. (2022). IEEE Standard for Data Privacy Process (IEEE Std 7002-2022). IEEE Computer Society

23. Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. Information, Communication &Society, 22(1), 65-98

24. Ibrahim, Ekhlas Mokhles, Ziyad Tariq Jassi,2025, Tort liability for Dealing with Personal Data in The Digital Environment, 9th International Legal Issues Conference (ILIC9), pp.1-7.

25. Kaddouri, Rym Fatiha,2024, Privacy Awareness and its Importance for Social Media Users an Exploratory Study of Facebook Users in the Arab World,252-253.

26. Koynja,2024, The Legal Implications of Data Protection Laws, AI Regulation, and Cyber security Measures on Privacy Rights in 2024, Global International Journal of Innovative Research

27. Krause, M., Grant, S., & Moore, L. (2021). Human factors in university data breaches: A case study of Australian higher education. Journal of Cybersecurity Education.

28. Kwon, J. (2023). A Study on Ethical Awareness Changes and Education in Artificial Intelligence Society. Revue d' Intelligence Artificially, 37(2), 341-345.

29. MaMdoh Ameera,2023, Encyclopedia of Arabic Education: HBMSU, P.57

30. Masah Fatima,2024, E-Learning and the Smart University, Al-Rawaq Journal for scientific research among faculty members in Saudi public universities. International Journal of Educational and Psychological Sciences, 7(2), 15-45

10. Al-Sagheer, M. M. (2024). The legal nature of digital privacy: A study to clarify the regulations governing personal data protection via digital technology, Paper presented at the 8th Scientific Conference of the College of Law: "Legal Challenges in the Digital Age", Sultan Qaboos University, Sultanate of Oman**,** PP.311-339.

11. Al-shabata, Mohammed Ali Zaal, Al Wahsha Ziad Mohammad,2025, The Right to Privacy in the Digital Era, Al-Zaytoonah University of Jordan Journal for Legal studies, Volume (6), Issue (3), p.71

12. Al-Shahwani, M., & Al-Qahtani, A. (2022). The reality of digital competencies among technical employees in Saudi universities. Arab Journal of Educational and Psychological Sciences, 7(2), 15

13. Al-Shaya, A. M. (2021). Smart Universities: Analysis and Evaluation. Dar Al-Fikr Al-Arabi, P.45

14. Aziz, Ali Salem,2026, Digital Transformation and Protection of Personal Data of Students and Employees in Iraqi Universities, Al-Haqooq Journal.PP.1-8.

15. ben aida Fauziya, Bahsosee rekia, Data governance in higher education institutions, Al-Maghrebi Journal of Manuscripts vol20(1), pp155-190.

16. Ben mansour nassima,2025, The Contributions of the Smart University to the Development of the Educational Process,contact Journal,Vol.31,No.4,150-151.

17. Ben zakaria Yacine otmane, ,2021, The problem of digital ethics of the digital citizen in the virtual public domain)Standards and tools, Al-Riwaq Journal for Social and Humanitarian Studies,Vol.7,No.1,208-227)

18. Camilleri, M. A. ,2023," Artificial intelligence governance: Ethical considerations and implications for social

aconceptual framework structured review and research agenda" , International Journal of Information Management (IJIM),]university of Liechtenstein, p.11

37. Sultan Hikmat Rasheed,2020 , Towards Smart Universities Through Adopting University Governance Standards: A Study in a Sample of Private Universities in Duhok City, Academic Journal of Nawroz University, 9(2):310

38. Pham bich Thuy & Pham Dao Tien,2025, Smart Administration as the Backbone of the smart University: A Conceptual, P.72 framwork, IJCESEN, Vol1, No.3Gurdiannew,201

39. Tufakg, Haytham Khalil,2026, Educational Data governance and its Role in Raising the Efficiency of School Administration: A Proposed Model for Public Schools, Journal of Educational and Psychological Sciences (JEPS), Vol. 10, Issue3, P: 118 – 109.

40. Vadym Kaptur (2019), "Smart Universities are the basis for the development of sustainable cities، Forum on Smart sustainable cities: technological trends", success stories and future prospects" Minsk, Belarus, P90.

Social and Human Studies، Vol.11(1), PP 358-372.

31. Mauro Coccoli &Angela Guercio &Paolo Maresca &Lidia Stanganelli, 2014, Smarter universities: A vision for the fast-changing digital era. Journal of Visual Languages & Computing ،1003-1011

32. Matthew N. O. Sadiku, 2Yogita P. Akhare, Abayomi Ajayi-Majebi and 4Sarhan M. Musa, Smart University: An Introduction, International Journal of Trend in Research and Development, Volume 7(3),2020.

33. Mehdi, Essaghir Mohammed,2024, The Legal Nature of Digital Privacy: A Study of the Regulatory Provisions for Personal Data Protection via Digital Technology, 8th Scientific Conference of the College of Law, Sultan Qaboos University,319

34. Miller, Vincent,2011, Understanding digital culture, Convergence and the contemporary media experience, London: Sage Publications, P 102.

35. Reema Ahmad Alharb,2026, The Right to Privacy in the Age of Artificial Intelligence, International Journal of Low Research and Studies (IJLRS), Vol.5, No.5, P.14.

36. Rene abraham, Jan vom brocke, Johannes Schneider,2019,"Data governance: