حماية البيانات والخصوصية في البيئة الرقمية: دراسة مقارنة بين جامعة كاليفورنيا بيركلى وجامعة عين شمس

Data Protection and Privacy in the Digital Environment: A Comparative Study between the University of California, Berkeley and Ain Shams University

إعداد

أميرة صبري أحمد رياض

مستخلص البحث

يهدف هذا البحث إلى دراسة الإطار النظري لحماية البيانات والخصوصية في البيئة الرقمية، باعتبارها قضية محورية تزداد أهميتها في المؤسسات الأكاديمية مع تسارع وتيرة التحول الرقمي، وقد أولت الأدبيات التربوية المعاصرة اهتمامًا واسعًا بهذا الموضوع لما يرتبط به من أثر مباشر في جودة البحث العلمي وضمان نزاهة الممارسات الأكاديمية. وفي هذا الإطار، يتناول البحث تجربة جامعة كاليفورنيا بيركلي بوصفها نموذجًا بارزًا على المستوى العالمي في تبني سياسات متقدمة لحماية البيانات الرقمية، حيث استطاعت أن تضع استراتيجيات متكاملة تسهم في رفع كفاءة أمن المعلومات وتوفير بيئة بحثية آمنة لكل من الطلاب وأعضاء هيئة التدريس، ويرتكز البحث على المنهج المقارن لتحليل أوجه التشابه والاختلاف بين جامعة كاليفورنيا بيركلي وجامعة عين شمس، بما يتيح تحديد عناصر القوة والفرص المتاحة إلى جانب التحديات التي تواجه كل منهما، وصولًا إلى استخلاص الدروس المستفادة وصياغة آليات مقترحة لتعزيز سياسات حماية البيانات والخصوصية في الجامعات المصرية، ويهدف البحث في محصلته النهائية إلى دعم الأمن المعلوماتي وتحسين

مستوى الأداء البحثي، فضلًا عن الإسهام في تطوير البنية التحتية الرقمية على نحو يتناسب مع متطلبات التعليم العالي في العصر الحديث.

الكلمات المفتاحية :**حماية البيانات، الخصوصية الرقمية، التعليم العالي.**

Abstract:

his research aims to examine the theoretical framework of data protection and privacy in the digital environment, as it represents a central issue of growing importance for academic institutions amid the accelerating pace of digital transformation. Contemporary educational literature has devoted considerable attention to this subject due to its direct impact on the quality of scientific research and the integrity of academic practices. Within this context, the study explores the experience of the University of California, Berkeley, as a prominent global model in adopting advanced policies for digital data protection, having succeeded in developing comprehensive strategies that enhance information security and provide a safe research environment for both students and faculty members. The research adopts a comparative methodology to analyze the similarities and differences between the University of California, Berkeley, and Ain Shams University, thereby identifying strengths, opportunities, and challenges faced by each institution. Based on this analysis, the study seeks to draw valuable lessons and propose mechanisms to strengthen data protection and privacy policies in Egyptian universities. Ultimately, the research aims to reinforce information security, improve the quality of research performance, and contribute to the development of digital infrastructure in line with the requirements of higher education in the modern era.

Keywords: Data protection, digital privacy, **Higher Education**.

اولاً: الإطار العام للبحث

مقدمة البحث

يشهد العالم المعاصر ثورة رقمية غير مسبوقة جعلت من البيانات والمعلومات محورًا أساسيًا في مختلف القطاعات، ولا سيما في المؤسسات الأكاديمية. فقد تجاوزت الجامعات دورها التقليدي في التعليم والبحث العلمي لتتحول إلى بيئات رقمية متكاملة تعتمد على تقنيات متقدمة مثل نظم إدارة التعلم، والحوسبة السحابية، والذكاء الاصطناعي في تحليل البيانات الضخمة. ومع هذا التحول، أصبحت قضايا حماية البيانات والخصوصية من أبرز التحديات التي تواجه هذه المؤسسات، نتيجة التعامل مع كميات هائلة من البيانات الحساسة الخاصة بالطلاب وأعضاء هيئة التدريس والباحثين، الأمر الذي يستلزم تطوير آليات فعّالة لحوكمة البيانات وبناء الثقة وضمان الامتثال للقيم المؤسسية (Maltese, 2024, 242).

وفي هذا الإطار، يُعد نموذج **جامعة كاليفورنيا بيركلي** مثالًا رائدًا عالميًا في تطبيق معايير الأمن السيبراني وحوكمة البيانات، حيث تتبنى استراتيجيات متقدمة تستند إلى الأطر التشريعية الدولية مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR) والتشريعات الفيدرالية الأمريكية، بما يضمن مستويات عالية من الامتثال وحماية الخصوصية. ويعزز هذا التوجه دور مكتب الأخلاقيات والمخاطر والامتثال (OERCS) الذي يشرف على عدد من اللجان الرئيسة مثل لجنة الامتثال والمخاطر المؤسسية (CERC)، ولجنة حوكمة مخاطر المعلومات (IRGC)، ولجنة حوكمة البيانات (DGC)، بالإضافة إلى الفريق المنسق للمراجعة المجتمعية (CCRT)، بما يسهم في إرساء إطار مؤسسي متكامل لتحقيق التوازن بين الأمن والخصوصية وإدارة المخاطر والسياسات بكفاءة (UC Berkeley, 2025, https://oercs.berkeley.edu/about).

ولا يقتصر نجاح سياسات الحماية على التشريعات واللوائح المؤسسية فحسب، بل يرتبط أيضًا بتنمية الوعي الأمني وتعزيز ثقافة حماية البيانات بين أفراد المجتمع الأكاديمي. فالممارسات اليومية البسيطة مثل استخدام كلمات مرور قوية، وتفعيل المصادقة الثنائية، والالتزام بسياسات الاستخدام الآمن، تمثل خط الدفاع الأول ضد الهجمات الإلكترونية. وقد أكدت الدراسات الحديثة أن بناء بيئة أكاديمية آمنة لا يعزز الثقة بين جميع الأطراف المشاركة في العملية التعليمية فحسب، بل يدعم أيضًا استدامة البحث العلمي والتحول الرقمي والتعليم الرقمي **(Farayola et al., 2024, 607)**.

مشكلة البحث

تواجه الجامعات المصرية تحديات متزايدة في مجال حماية البيانات والخصوصية نتيجة ضعف البنية التحتية للأمن السيبراني وغياب السياسات الواضحة لتنظيم الوصول إلى المعلومات الحساسة، الأمر الذي يرفع من احتمالية الاختراقات وتسرب البيانات. ومع استمرار التحول الرقمي، يواجه الباحثون صعوبة في حماية بياناتهم الأكاديمية من التهديدات الإلكترونية مثل الاختراق والتسريب، وهو ما ينعكس سلبًا على موثوقية الأبحاث وسلامتها، خاصة في ظل محدودية التدابير الأمنية المتاحة **(على، عبير أحمد، ٢٠٢٠، ١٧٦)**.

ورغم التوسع في الاعتماد على تقنيات رقمية مثل التخزين السحابي وتحليل البيانات عبر الإنترنت، لا تزال الجامعات تفتقر إلى استراتيجيات متكاملة تضمن أمن البيانات الأكاديمية وخصوصية المشاركين في الدراسات البحثية. ويُعزى ذلك إلى قصور البنية التكنولوجية وعدم ملاءمتها للتحديات المتسارعة في أمن المعلومات، مما يستدعي تطوير سياسات أكثر صرامة إلى جانب تعزيز البرامج التدريبية لرفع

كفاءة الباحثين في التعامل مع متطلبات الأمان الرقمي (**أمين، مصطفى أحمد** ، ٢٠١٨، ٩٥).

كما تعاني الجامعات من ضعف في الامتثال للمعايير القانونية والأخلاقية المتعلقة بحماية البيانات، الأمر الذي يزيد من المخاطر السيبرانية على البحث العلمي، ويبرز الحاجة الملحة إلى إعادة تقييم وتطوير آليات الحماية بما يضمن بيئة أكاديمية آمنة وموثوقة (**جمهورية مصر العربية رئاسة مجلس الوزراء المجلس الأعلى للأمن السيبراني** ، ٢٠١٧، ٥)، وتواجه المكتبات الرقمية بدورها تحديات مشابهة، حيث يشكل غياب السياسات الشاملة وضعف تطبيق تقنيات التشفير والتحقق من الهوية تهديدًا لسرية المعلومات ويؤثر على ثقة الباحثين في استخدامها(**يس، إيمان عبدالحميد، و السيد، أماني محمد**، ٢٠٢٢، ١٦٨).

وفي ضوء ذلك، يصبح من الضروري تبني سياسات متكاملة لحماية البيانات والخصوصية داخل الجامعات المصرية، بما يتوافق مع التشريعات الوطنية والمعايير الدولية، بهدف إنشاء بيئة بحثية رقمية آمنة تضمن أمن المعلومات وسلامة الأبحاث الأكاديمية، تأسيسًا على ما سبق يحاول البحث الإجابة عن السؤال الرئيس التالي:-

"كيف يتم تعزيز حماية البيانات والخصوصية في البيئة الرقمية بالجامعات المصرية على ضوء خبرة جامعة كاليفورنيا بيركلي؟"

ويمكن صياغة السؤال الرئيس في الأسئلة الفرعية التالية:-

١. ما الإطار النظري لحماية البيانات والخصوصية في البيئة الرقمية بالجامعات في الأدبيات التربوية المعاصرة؟

٢. ما أبرز سياسات حماية البيانات والخصوصية في البيئة الرقمية بجامعة كاليفورنيا بيركلي بالولايات المتحدة الأمريكية في ضوء القوى والعوامل الثقافية المؤثرة؟

٣. ما واقع سياسات حماية البيانات والخصوصية في البيئة الرقمية بجامعة عين شمس في مصر في ضوء القوى والعوامل الثقافية المؤثرة؟

٤. ما أوجه التشابه والاختلاف بين جامعة كاليفورنيا بيركلي بالولايات المتحدة الأمريكية وجامعة عين شمس في مصر فيما يتعلق بسياسات حماية البيانات والخصوصية في البيئة الرقمية داخل الجامعات؟

٥. ما الآليات المقترحة لتطوير استراتيجيات حماية البيانات والخصوصية في الجامعات المصرية، استنادًا إلى خبرة جامعة كاليفورنيا بيركلي وبما يتوافق مع احتياجات المجتمع المصري وسياقه الثقافي؟

اهداف البحث

١. تعريف الإطار النظري لحماية البيانات والخصوصية في البيئة الرقمية في الأدبيات التربوية المعاصرة.
٢. الاستفادة من دراسة جامعة كاليفورنيا بيركلي في تعزيز حماية البيانات والخصوصية في البيئة الرقمية بالجامعات.
٣. إجراء دراسة تحليلية مقارنة بين جامعة كاليفورنيا بيركلي وجامعة عين شمس، وتحديد أوجه التشابه والاختلاف في سياسات حماية البيانات والخصوصية.
٤. التوصل إلى مجموعة من المقترحات لتطوير استراتيجيات حماية البيانات والخصوصية في الجامعات المصرية، استنادًا إلى تجربة جامعة كاليفورنيا بيركلي وبما يتوافق مع احتياجات المجتمع المصري.

اهمية البحث: اكتسب البحث الحالى اهميته من حيث:-

- **تحديد التحديات التي يواجهها الباحثون في الجامعات المصرية في ظل غياب أو ضعف تدابير حماية البيانات والخصوصية الرقمية.**
- **تقديم حلول مبتكرة لتطوير استراتيجيات حماية البيانات وتعزيز استخدام الأدوات الرقمية في البحث الأكاديمي.**
- **مساعدة الجامعات المصرية في تحديد احتياجاتها الفعلية في مجال حماية البيانات الرقمية والبرامج التدريبية التي تضمن التمكين الرقمي للباحثين.**

حدود البحث

- حدود موضوعية: **سياسات حماية البيانات والخصوصية في البيئة الرقمية داخل الجامعات.**
- حدود مكانية: **اقتصرت الدراسة على الواقع الفعلي لسياسات حماية البيانات والخصوصية في الجامعات المصرية، مع الاستفادة من خبرة جامعة كاليفورنيا بيركلي بالولايات المتحدة الأمريكية باعتبارها نموذجًا عالميًا رائدًا في هذا المجال.**
- حدود بشرية: **اقتصرت الدراسة على الباحثين بالجامعات، وتشمل أعضاء هيئة التدريس، الهيئة المعاونة، وطلاب الدراسات العليا.**

خطوات السير في البحث

١. **تقديم الإطار العام للبحث.**

٢. عرض الإطار النظري للبحث، ويتضمن ثلاثة محاور رئيسة: مفهوم حماية البيانات والخصوصية في البيئة الرقمية، والأطر القانونية والأخلاقية المرتبطة بها، بالإضافة إلى التحديات المتعلقة بخصوصية وأمن البيانات في البيئة الرقمية.

٣. تحليل سياسات حماية البيانات والخصوصية في البيئة الرقمية بجامعة كاليفورنيا بيركلي بالولايات المتحدة الأمريكية، في ضوء القوى والعوامل الثقافية المؤثرة.

٤. دراسة واقع سياسات حماية البيانات والخصوصية في البيئة الرقمية بجامعة عين شمس في مصر، في ضوء القوى والعوامل الثقافية المؤثرة.

٥. استخلاص أوجه التشابه والاختلاف بين جامعتي كاليفورنيا بيركلي وعين شمس فيما يتعلق بسياسات حماية البيانات والخصوصية في البيئة الرقمية الجامعية.

٦. اقتراح آليات لتطوير استراتيجيات حماية البيانات والخصوصية في الجامعات المصرية، بالاستفادة من خبرة جامعة كاليفورنيا بيركلي، وبما يتناسب مع خصوصية المجتمع المصري وسياقه الثقافي.

منهج البحث

استخدمت الباحثة المنهج المقارن في تناول استراتيجيات حماية البيانات والخصوصية بجامعتي كاليفورنيا بيركلي في الولايات المتحدة الأمريكية وعين شمس في مصر، باعتباره الأنسب بين مناهج التربية المقارنة والأكثر شمولًا في استيعاب المناهج الفرعية المرتبطة بها. ويسير البحث وفق خطوات المنهج المقارن على النحو التالي:-

- **موضوع الدراسة (مشكلة البحث وغرضه):** تمثلت المشكلة في وجود قصور في استراتيجيات حماية البيانات والخصوصية داخل الجامعات المصرية، أما

الغرض فيكمن في الوقوف على واقع هذه الاستراتيجيات في جامعة عين شمس، بالاستفادة من خبرة جامعة كاليفورنيا بيركلي، وصولًا إلى صياغة توصيات عملية تسهم في تطويرها ومعالجة التحديات القائمة.

- **الإطار الأيديولوجي:** تمثل في وصف وتحليل استراتيجيات حماية البيانات والخصوصية في الجامعتين محل الدراسة، بما يوضح السياقات التي أظهرت المشكلة.
- **تفسير الظواهر:** اعتمد على الربط بين المشكلات المرتبطة بالموضوع في كلتا الجامعتين، وتحليل أبعادها.
- **المقارنة:** أجريت مقارنة منهجية بين الظاهرة محل الدراسة في الجامعتين، بعد وصفها وتحليلها.
- **التعميم:** استخلاص أوجه التشابه والاختلاف، وتفسيرها في ضوء القواعد العامة التي تحكم الظاهرة، بما أتاح بناء إطار مرجعي يمكن الاستناد إليه عند صياغة التوصيات والرؤى المستقبلية.
- **التنبؤ:** باعتباره ثمرة التربية المقارنة، فقد سعت الدراسة إلى رسم صورة مستقبلية لاستراتيجيات حماية البيانات والخصوصية في الجامعات المصرية، استنادًا إلى التحليل المقارن، بعيدًا عن الحدس والتخمين، وبما يدعم التوجه نحو سياسات أكثر فاعلية.

مصطلح حماية البيانات والخصوصية في البيئة الرقمية تنفيذ إجراءات وتقنيات تضمن أمن المعلومات الشخصية والمؤسسية، مع الالتزام بالمعايير القانونية والتنظيمية، ويعد التوازن بين إتاحة البيانات واستخدامها بشكل آمن تحديًا مستمرًا، يتطلب وعيًا مستمرًا وتطويرًا متواصلًا للسياسات الأمنية للحفاظ على الخصوصية في

العالم الرقمي **(O'Toole, E., Feeney, L., Heard, K., & Naimpally, R. , 2018, 3).**

ونُعرِّف حماية البيانات والخصوصية في البيئة الرقمية إجرائيًا بأنها مجموعة من الإجراءات والتقنيات المطبَّقة لضمان أمان المعلومات الشخصية والمؤسسية في الفضاء الرقمي، ويتضمن ذلك اعتماد سياسات أمنية تتوافق مع المعايير القانونية والتنظيمية لمنع الوصول غير المصرح به أو التسريب أو الاختراق، ويهدف هذا إلى ضمان الاستخدام الآمن للبيانات مع الحفاظ على الخصوصية، وهو ما يستدعي تطويرًا مستمرًا للأنظمة الأمنية، إلى جانب رفع مستوى وعي المستخدمين بكيفية التعامل مع المعلومات الرقمية بما يحفظ حقوق الأفراد ويصونها.

الدراسات السابقة

اولًا : الدراسات العربية.

١. دراسة **(إيمان عبدالحميد& أماني محمد،**٢٠٢٢ م) بعنوان حماية البيانات الشخصية بالمكتبات الجامعية في مصر: دراسة استكشافية **(يس، إيمان عبدالحميد، و السيد، أماني محمد** ، ٢٠٢٢، ١٥٣ – ١٧٠).

هدفت الدراسة التعرف على السياسات التي تتبعها المكتبات الجامعية المصرية سواء مكتبات الجامعات الحكومية أو الخاصة ومدي ملائمة تلك السياسات مع قانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، وتأتي أهمية هذه الدراسة في كونها من أولى الدراسات التي تلقي الضوء على السياسات المتبعة في قطاع المكتبات لحماية البيانات الشخصية ومدي توافقها مع القانون المصري لحماية البيانات الشخصية، **واستخدمت الدراسة** المنهج المسحي الميداني الذي يتخذ من الأسلوب الوصفي التحليلي أداة له، **وتوصلت الدراسة** لمجموعة من النتائج من أبرزها أن ما يتم بالمكتبات الجامعية المصرية هي ممارسات لحماية البيانات الشخصية

للمستفيدين، حيث لا يوجد سياسة مكتوبة ومعلنة لدي المكتبات سواء بالجامعات الحكومية أو الخاصة.

٢. دراسة(عبير احمد على، ٢٠٢٠م) بعنوان سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية (**على، عبير أحمد** ، ٢٠٢٠، ١٣٣-٢٠٠).

هدفت الدراسة إلى اقتراح رؤية لإدماج سياسات الأمن السيبراني في الجامعات المصرية ضمن استراتيجية التحول الرقمي، مع التركيز على حماية البيانات والخصوصية في البيئة الأكاديمية، **واستخدمت الدراسة** المنهج الوصفي، وتناولت متطلبات التحول الرقمي، جهود الجامعات المصرية وتحدياتها، إضافة إلى مفهوم الأمن السيبراني وأهميته وسبل الحماية من المخاطر، **وتوصلت الدراسة** إلى ضرورة تبني سياسات فعالة لحماية البنية التحتية الرقمية للجامعات وتعزيز معايير الخصوصية، مما يسهم في تحسين أمن المعلومات، وضمان موثوقية البيانات الأكاديمية، وتعزيز تصنيف الجامعات عالميًا، ودعم دورها في التنمية الاقتصادية من خلال بيئة رقمية آمنة ومستدامة.

ثانيًا: الدراسات الأجنبية

١. دراسة(أولواتوين أيوك فاريولا، أولوبوكومي لطيفة، فيليب أولاسيني،٢٠٢٤م) حماية البيانات والخصوصية في تكنولوجيا المعلومات: مراجعة للتقنيات والتحديات" (Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. 2024, 606-615).

هدفت الدراسة إلي استعراض التقنيات والتحديات المرتبطة بحماية البيانات والخصوصية في نظم تكنولوجيا المعلومات، مع التركيز على أهمية التشفير والتحكم في الوصول لضمان أمن المعلومات، **واعتمدت الدراسة** على مراجعة الأدبيات العلمية لتحليل التهديدات الحالية واللوائح التنظيمية، **وتوصلت الدراسة** إلي أن حماية البيانات والخصوصية ضرورية لتعزيز الثقة المؤسسية، مما يستدعي تبني الجامعات تدابير أمنية فعالة لمواجهة التهديدات الرقمية المتزايدة.

٢. دراسة (ماري آن سمارت& دانيال تان،٢٠٢٢م) بعنوان تحديات حماية البيانات والخصوصية في أبحاث طلاب الدكتوراه بالجامعات .(Smart, M. A., & Tan, D ,2022, 3-4)

هدفت الدراسة إلى استكشاف التحديات التي يواجهها طلاب الدكتوراه في مجال حماية البيانات والخصوصية عند إجراء بحوث تشمل مشاركين من البشر، مع التركيز على قضايا مثل إخفاء الهوية، مشاركة البيانات بأمان، والامتثال للمعايير القانونية والتنظيمية، **واستخدمت الدراسة** المنهج النوعي جمع بين الاستطلاعات والمقابلات مع ١٨ طالبًا، **وتوصلت الدراسة** إلى أن الباحثين غالبًا ما يواجهون صعوبات بفهم متطلبات الامتثال وضمان سرية المعلومات الحساسة. وأوصت بضرورة تعزيز التوعية والتدريب على سياسات الأمان الرقمي لدعم بيئة بحثية آمنة تصون خصوصية الأفراد.

تعليق عام على الدراسات السابقة.

ناقشت الدراسات السابقة موضوع حماية البيانات والخصوصية من زوايا متعددة؛ حيث تناولت دراسات عربية واقع السياسات المتبعة في المكتبات الجامعية المصرية ومدى توافقها مع قانون حماية البيانات الشخصية (إيمان عبد الحميد & أماني محمد، ٢٠٢٢)، كما ركزت أخرى على وضع رؤية مقترحة لإدماج سياسات الأمن السيبراني في الجامعات المصرية في إطار التحول الرقمي (عبير أحمد علي، ٢٠٢٠). أما الدراسات الأجنبية فقد سلطت الضوء على التقنيات والتحديات المرتبطة بحماية البيانات في نظم تكنولوجيا المعلومات (Farayola et al., 2024)، إلى جانب التحديات العملية التي تواجه طلاب الدكتوراه في الجامعات عند التعامل مع قضايا الخصوصية والامتثال للمعايير القانونية (Smart & Tan, 2022).

ومن ثم، يستكمل البحث الحالي ما طرحته هذه الدراسات من خلال تناول سياسات حماية البيانات والخصوصية في البيئة الرقمية بالجامعات، مع التركيز على الجامعات المصرية ومقارنتها بخبرة جامعة كاليفورنيا بيركلي، وذلك بهدف اقتراح

آليات عملية لتطوير هذه السياسات بما يتلاءم مع احتياجات المجتمع الأكاديمي المصري.

ثانيًا: الإطار النظري للبحث

والذي يشمل على ثلاثة محاور:

- **مفهوم حماية البيانات والخصوصية في البيئة الرقمية.**

تُعد حماية البيانات والخصوصية في البيئة الرقمية من القضايا الجوهرية في العصر الرقمي، نظرًا لتعرض المعلومات لمخاطر متعددة مثل الاختراق، التسريب، والقرصنة الإلكترونية، وهو ما يفرض الحاجة إلى استراتيجيات أمنية متقدمة، وسياسات قادرة على ضمان سرية البيانات وسلامتها عند تداولها في الفضاء الرقمي، وتساهم المؤسسات التقنية والهيئات التنظيمية في هذا السياق من خلال توفير حلول تكنولوجية متطورة، ونشر الوعي بأهمية التدابير الوقائية، في حين تبرز مسؤولية الأفراد والمؤسسات في تبني ممارسات أمنية فعّالة كالتشفير، المصادقة متعددة العوامل، والتحديثات المستمرة لحماية البيانات من التهديدات السيبرانية.

ويُعرَّف **مفهوم حماية البيانات والخصوصية** في البيئة الرقمية بأنه مجموعة من الإجراءات والسياسات والتقنيات التي تُطبَّق لضمان أمن المعلومات الشخصية والمؤسسية، مع الالتزام بالمعايير القانونية والتنظيمية، ويعكس هذا المفهوم تحديًا مستمرًا يتمثل في الموازنة بين إتاحة البيانات واستخدامها بشكل آمن، بما يتطلب وعيًا متناميًا وتطويرًا دائمًا للسياسات الأمنية للحفاظ على الخصوصية في العالم الرقمي (O'Toole, E., Feeney, L., Heard, K., & Naimpally, R. ,2018, 3).

- **الأطر القانونية والأخلاقية لحماية البيانات.**

تُعد حماية البيانات في البيئة الرقمية ركيزة أساسية للحفاظ على خصوصية الأفراد وصون المعلومات الحساسة، الأمر الذي يفرض وجود أطر قانونية وأخلاقية واضحة تضمن التعامل الآمن مع البيانات، وتشمل هذه الأطر مبادئ أساسية مثل الاعتبارات الأخلاقية والموافقة المستنيرة، بما يضمن شفافية جمع البيانات ومعالجتها وإطلاع الأفراد على كيفية استخدامها.

كما تبرز أهمية الدور الرقابي للهيئات المختصة والسياسات الأمنية في متابعة أنظمة الحماية الرقمية وضمان الالتزام بالمعايير المعتمدة، وتأتي التشريعات الدولية مثل اللائحة العامة لحماية البيانات (**GDPR**) نموذجًا رائدًا في هذا المجال، حيث تحدد حقوق الأفراد، وتنظم طرق تخزين البيانات واستخدامها، وتفرض عقوبات رادعة على الانتهاكات، بما يعزز الأمن والخصوصية في الفضاء الرقمي (Faster Capita ,2024, https://fastercapital.com/content/Confidentiality-in-research--Maintaining-Privacy-in-Scientific-Studies.html).

- **تحديات خصوصية وأمان البيانات فى البيئة الرقمية.**

تواجه حماية البيانات والخصوصية في البيئة الرقمية مجموعة من التحديات المعقدة، حيث يُعد الوصول إلى البيانات ومشاركتها بين المؤسسات البحثية مقيدًا بالإجراءات الإدارية الصارمة، مما يعيق التعاون العلمي الفعال، كما يُمثل ضمان إخفاء الهوية عقبة رئيسية، خصوصًا عند التعامل مع مجموعات بيانات صغيرة، إذ يتطلب الأمر تقنيات متقدمة وجهودًا إضافية لتفادي إعادة التعرف على الأفراد. إلى جانب ذلك، تظهر مخاوف أخلاقية وقانونية عند توظيف المشاركين، خاصة الفئات الحساسة، مما يستلزم آليات رقمية آمنة تعزز الشفافية والثقة.

كما يتضح أن غياب الوضوح القانوني والارتباك التقني يعرقل الامتثال للوائح مثل الـGDPR والقوانين المحلية، وهو ما يضاعف العبء الإداري على الباحثين، وتبرز تحديات أخرى مرتبطة بالبنية التحتية التقنية، مثل ضعف أنظمة التخزين الآمن أو الاعتماد على أجهزة شخصية غير محمية، مما يزيد من احتمالية فقدان البيانات أو تعرضها للاختراق. إلى جانب ذلك، لا يزال الأمن المادي يُشكل بُعدًا مهمًا في حماية البيانات، مما يتطلب حلولًا متكاملة تجمع بين الحماية الرقمية والواقعية.

وتتعمق هذه التحديات بفعل فجوات التدريب ونقص الوعي لدى الباحثين وفرق العمل البحثية، إلى جانب ديناميكيات القوة داخل الفرق التي قد تُهمِل الجوانب المرتبطة بالخصوصية، كما أن الضغوط الأكاديمية والاجتماعية على سرعة الإنجاز قد تُضعف الالتزام بالمعايير الأمنية، وهو ما يستدعي تعزيز برامج التدريب المتخصصة، وتبني استراتيجيات مؤسسية متوازنة تحقق الإنتاجية البحثية دون الإخلال بمبادئ حماية البيانات والخصوصية (Smart, M. A., & Tan, D ,.2022, 3-4)

يتضح مما سبق أن حماية البيانات والخصوصية في البيئة الرقمية لا تقتصر على كونها التزامًا أخلاقيًا أو قانونيًا، بل تمثل ركيزة أساسية في تعزيز جودة الأبحاث العلمية، من خلال ضمان أمن المعلومات، يتمكن الباحثون من بناء الثقة مع المشاركين، وتحسين دقة البيانات، والالتزام بالمعايير الأخلاقية، مما يؤدي إلى نتائج علمية أكثر موثوقية وقابلة للتطبيق. كما يُسهم ذلك في رفع كفاءة الباحثين، وتعزيز تأثير أبحاثهم في المجال العلمي، مع ضمان توافقها مع معايير الأمان والخصوصية في البيئة الرقمية المتطورة.

ثالثًا: حماية البيانات والخصوصية في البيئة الرقمية بجامعة كاليفورنيا بيركلي

تُعد جامعة كاليفورنيا، بيركلي من الجامعات الرائدة عالميًا، حيث احتلت المرتبة الثامنة وفق تصنيف "تايمز للتعليم العالي" لعام ٢٠٢٥م، (Times Higher Education ,2025, https://www.timeshighereducation.com/world-university-rankings/university-california-berkeley). كما صُنفت ، أفضل جامعة حكومية ورابع أفضل جامعة على مستوى العالم وفقًا لتقرير "يو إس نيوز آند وورلد ريبورت" (IEP , 2025, https://iep.berkeley.edu/content/uc-berkeley-rated-number-one-public-university-world-and-fourth-best-overall-us-news) ، ومع التوسع المتسارع في التحول الرقمي، برزت حماية البيانات والخصوصية في النشر الأكاديمي كأولوية استراتيجية للجامعة، بما يضمن بيئة بحثية آمنة ومتوازنة بين الانفتاح العلمي وصون الملكية الفكرية.

وفي هذا السياق، تبنت الجامعة سياسات متقدمة وإجراءات تنظيمية دقيقة لحماية البيانات الشخصية والبحثية، مع توفير إرشادات شاملة للباحثين لضمان الامتثال لمعايير الخصوصية، وتسعى بيركلي إلى تحقيق التكامل بين إتاحة الوصول المفتوح إلى المعرفة وبين صيانة حقوق المؤلفين والباحثين، خاصة مع تعاظم تحديات تقنيات جمع البيانات وتتبع المستخدمين في البيئة الرقمية.

ويُعد برنامج **دعم البحث مع حماية خصوصية الباحثين (SCIP)** أحد أبرز المبادرات في هذا المجال، حيث يوفّر إطارًا مؤسسيًا يدعم النشر المفتوح وإدارة البيانات البحثية مع الحفاظ على سرية المعلومات الأكاديمية، كما يقدم البرنامج خدمات استشارية متخصصة حول حقوق النشر والاستخدام العادل، ويُسهم في

تطوير سياسات مؤسسية ووطنية ودولية تحمي حقوق الباحثين وتعزز فرص الاكتشاف العلمي الآمن، وإلى جانب ذلك، يركز البرنامج على رفع وعي المجتمع الأكاديمي بأحدث الاتجاهات في الاتصال العلمي، وضمان التزام عمليات جمع البيانات وتحليلها بأعلى معايير الأمان، بما يعزز استدامة بيئة البحث العلمي الرقمية (Berkeley Library , 2025, https://www.lib.berkeley.edu/research/scholarly-communication/about).

سياسات حماية البيانات والخصوصية في جامعة كاليفورنيا بيركلي

تتبنى جامعة كاليفورنيا بيركلي منظومة متكاملة من السياسات المؤسسية لحماية البيانات والخصوصية، مستندة إلى **أطر قانونية دولية ووطنية** مثل **GDPR** (اللائحة العامة لحماية البيانات الأوروبية)، و**HIPAA** (قانون قابلية التأمين الصحي والمساءلة في الولايات المتحدة)، و**FERPA** (قانون خصوصية السجلات التعليمية للطلاب)، وتهدف هذه السياسات إلى ضمان أمن المعلومات الشخصية والبحثية، ومنع الوصول غير المصرح به إليها، بما يعكس التزام الجامعة بالمسؤولية الأخلاقية والقانونية في إدارة البيانات في البيئة الأكاديمية الرقمية (Berkeley Library ,2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright).

في مجال **النشر العلمي**، تركز السياسات على حماية الباحثين وبياناتهم عبر مجموعة من الإجراءات الوقائية، من أبرزها: إزالة البيانات الوصفية من الملفات البحثية قبل مشاركتها، الاعتماد على مستودعات رسمية مثل **eScholarship** بدلاً من المنصات التجارية، واستخدام أدوات تكنولوجية تعزز الخصوصية مثل الشبكات الافتراضية الخاصة (**VPN**) ومتصفحات آمنة لمنع التتبع، كما تُشدد الجامعة على

الالتزام الصارم بشروط استخدام المنصات الأكاديمية وتجنب الإفصاح عن أي بيانات حساسة دون موافقة مسبقة (Berkeley Library ,2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright).

وتولي بيركلي أهمية خاصة لتحقيق التوازن بين **الوصول المفتوح وحماية الملكية الفكرية**. ولهذا الغرض، توصي باستخدام تراخيص **Creative Commons** المناسبة لضمان حقوق الباحثين، مع التحذير من منصات النشر غير الموثوقة التي قد تستغل البيانات البحثية، كما تتيح السياسات للباحثين الاحتفاظ بحقوق مؤلفاتهم عند التفاوض مع الناشرين، مما يعزز استقلاليتهم الأكاديمية ويحافظ على سرية بياناتهم (Berkeley Library ,2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright).

وفيما يخص **مراجعة الأقران**، تعتمد الجامعة سياسة المراجعة "**مزدوجة التعمية**" لضمان سرية هوية المؤلفين والمراجعين، ومنع أي استخدام غير مشروع للبيانات البحثية، ومع تزايد الاعتماد على تقنيات الذكاء الاصطناعي في البحث العلمي، تضع الجامعة ضوابط واضحة للاستخدام الأخلاقي لهذه الأدوات، بما في ذلك تشفير البيانات الحساسة، إخفاء الهوية، واستشارة اللجان الأخلاقية قبل إجراء التحليلات (Berkeley Library ,2025, https://www.lib.berkeley.edu/research/scholarly-communication/publishing).

كما تؤكد السياسات على أهمية الالتزام بمبادئ **الاستخدام العادل**، من خلال تنظيف البيانات الوصفية من المستندات البحثية، استخدام مستودعات موثوقة،

وتجنب مشاركة المعلومات عبر قنوات غير آمنة، ويمتد هذا الالتزام إلى اختيار المجلات الأكاديمية، حيث يُشترط مراجعة سياساتها المتعلقة بالخصوصية وحقوق النشر، مع الاعتماد على مؤشرات مثل **DOAJ** و**OASPA** لضمان موثوقية الناشر وتفادي المجلات المفترسة (Berkeley Library, 2025, at https://www.lib.berkeley.edu/research/scholarly-communication/copyright).

وعلى المستوى الدولي، عززت الجامعة ريادتها من خلال المشاركة في تطوير **بروتوكول بيركلي بالتعاون مع الأمم المتحدة**، والذي يمثل إطارًا قانونيًا وأخلاقيًا لاستخدام الأدلة الرقمية في التحقيقات الحقوقية، ويراعي هذا البروتوكول مبادئ حماية البيانات وحقوق الإنسان، بما يضمن التوازن بين الاستفادة من التكنولوجيا وحماية الخصوصية (الامم المتحدة حقوق الانسان ،٢٠٢٠،

https://www.ohchr.org/ar/stories/2020/12/berkeley-protocol-gives-guidance-using-public-digital-info-fight-human-rights) .

وأخيرًا، تُدمج جامعة كاليفورنيا بيركلي سياسات حماية البيانات في جميع مراحل **دورة حياة النشر الأكاديمي**، بما يضمن الامتثال للأطر القانونية مثل **GDPR** و**HIPAA**. ففي مرحلة **الإنشاء** يتم تأمين البيانات عبر التشفير، وفي **التقييم** تُحفظ سرية مراجعة الأقران، بينما تركز **مرحلة النشر** على إزالة البيانات الوصفية من الملفات البحثية، أما في **التوزيع وإتاحة الوصول**، فتلتزم الجامعة باستخدام مستودعات تحترم الخصوصية، في حين تعتمد مرحلة **الحفظ** على أنظمة مؤمنة تضمن استمرارية الوصول الآمن، وأخيرًا، تراعي مرحلة **إعادة الاستخدام** مبادئ الاستخدام العادل وحماية الخصوصية، وبهذا النهج، تقدم بيركلي نموذجًا متكاملًا يجمع بين تعزيز الانفتاح العلمي وصون أمن البيانات وخصوصية الباحثين

(Berkeley Library ,2025, https://www.lib.berkeley.edu/research/scholarly-communication/publishing).

دورة حياة النشر وحماية البيانات

وتُترجم هذه السياسات إلى ممارسات عملية تشمل عدة محاور تطبيقية؛ إذ تؤكد على الاستخدام المسؤول للذكاء الاصطناعي في الأبحاث مع مراعاة الجوانب القانونية والأخلاقية وحماية البيانات الحساسة، كما تتيح لطلاب الدراسات العليا الاحتفاظ بحقوق الطبع والنشر لأطروحاتهم مع إمكانية تقييد الوصول لحماية خصوصية البيانات أو تلبية متطلبات النشر المستقبلي (Berkeley Library , 2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright)، وبالمثل، تشدد الجامعة على أهمية اختيار المجلات ودور النشر الأكاديمية الموثوقة التي تلتزم بمعايير حماية البيانات والانفتاح العلمي المسؤول، ومن خلال هذا التكامل بين السياسات العامة والتطبيقات العملية، تسعى بيركلي إلى صياغة نموذج متوازن يجمع بين تعزيز الوصول إلى المعرفة

والحفاظ علي حقوق الباحثين وخصوصية بياناتهم في البيئة الرقمية، ويتجسد هذا التوجه عبر تبني سياسات صارمة لحماية البيانات، وإصدار إرشادات دقيقة للنشر الآمن، بما يضمن بيئة بحثية موثوقة تُعزّز الانفتاح العلمي مع الحفاظ على سرية المعلومات الأكاديمية.

القوى والعوامل الثقافية المؤثرة

تتأثر سياسات حماية البيانات والخصوصية في الولايات المتحدة الأمريكية بالعديد من العوامل الثقافية والتكنولوجية والاقتصادية المتداخلة، فعلى **المستوى الثقافي والاجتماعي**، يتضح أن وعي المجتمع الأمريكي بأهمية الخصوصية الرقمية شكّل أساسًا لبلورة تشريعات صارمة مثل اللائحة العامة لحماية البيانات (GDPR) وقانون(HIPAA)

(GDPR,2018,https://www.into.ie/app/uploads/2019/10/GDPR_FAQ.pdf)، بما انعكس على السياسات المؤسسية في الجامعات، ومن أبرزها جامعة كاليفورنيا بيركلي. وقد تبنت الجامعة ممارسات تعزز قيم الشفافية والحقوق الفردية، مثل النشر المفتوح، وتراخيص Creative Commons، وآليات المراجعة المزدوجة التعمية، بما يرسخ ثقافة المسؤولية الأخلاقية في إدارة البيانات

(Berkeley Library , 2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright)

ومن **الناحية التكنولوجية**، يُعد مستوى التطور الرقمي عاملاً جوهريًا في فهم سياسات حماية البيانات بجامعة كاليفورنيا بيركلي. إذ تتميز بيركلي ببنية تحتية رقمية متقدمة توفر بيئة تعليم إلكتروني آمنة، مدعومة بأنظمة متطورة لحماية بيانات

المستخدمين، ويُعزَّز هذا التوجه من خلال تشجيع المنتسبين على استخدام أدوات تقنية داعمة للخصوصية مثل متصفحي **Firefox** و**Brave**، مما يقلل من فرص التتبع الرقمي ويعزز ثقة الطلاب والباحثين في منظومة التعليم الإلكتروني (Berkeley Library, 2025, https://www.lib.berkeley.edu/research/scholarly-communication/copyright).

كما يمتد أثر هذا التقدم التكنولوجي إلى استراتيجيات إدارة البيانات، حيث تعتمد الجامعة على تقنيات الذكاء الاصطناعي والتعلم الآلي للكشف المبكر عن التهديدات الأمنية، وتستند إلى مستودعات بحثية رقمية متطورة مثل **eScholarship** لضمان حماية وسرية الأبحاث الأكاديمية، بما يعكس تكاملاً بين الابتكار التكنولوجي والسياسات المؤسسية في تعزيز أمن البيانات الأكاديمية.

رابعًا: حماية البيانات والخصوصية فى البيئة الرقمية بجامعة عين شمس

تولي جامعة عين شمس أهمية استراتيجية لحماية البيانات والخصوصية في ظل التحول الرقمي الذي يشهده التعليم العالي والبحث العلمي، حيث تسعى إلى ترسيخ بيئة بحثية آمنة وموثوقة تُعزز جودة المخرجات البحثية وتضمن نزاهتها، وتقوم سياسات الجامعة على نهج متكامل يجمع بين تبني أحدث تقنيات الأمن السيبراني والالتزام بالمعايير الأخلاقية والقانونية، بما يسهم في صون البيانات البحثية والمعلومات الأكاديمية من أي تهديدات سيبرانية أو انتهاكات محتملة.

سياسات حماية البيانات والخصوصية في جامعة عين شمس

تطبق الجامعة أنظمة أمن سيبراني متقدمة، **وتعمل من خلال برامج أكاديمية متخصصة على تأهيل كوادر بحثية قادرة على تطوير حلول متقدمة في مجال حماية البيانات والخصوصية، وتشمل هذه الجهود إعداد باحثين متخصصين في الأمن السيبراني عبر برامج تدريبية متطورة، إلى جانب دعم البحث التطبيقي في**

مجالات التشفير وتحليل البيانات الضخمة والذكاء الاصطناعي، كما تركز السياسات على مواكبة التطورات في الخصوصية الرقمية من خلال تحليل المخاطر الأمنية وتطوير آليات حديثة لحماية الهوية الرقمية وضمان سرية المعلومات، مع تعزيز التعاون البحثي على المستويين المحلي والدولي (Ain Shams University , 2025, https://chp-cis.asu.edu.eg/page/10#).

ويعكس **ميثاق السلوك الجامعي** بجامعة عين شمس التزامها المؤسسي بحماية الخصوصية (جامعة عين شمس، ٣٤،٢٠٢٥)، إذ يؤكد على مجموعة من المبادئ أبرزها: احترام سرية المعلومات الشخصية والبحثية، والحصول على موافقة مسبقة قبل استخدام البيانات أو الصور الخاصة بالأفراد، ومنع أي ممارسات تلاعب بالبيانات أو المحتوى الرقمي بما يحافظ على النزاهة البحثية (جامعة عين شمس ، ٢٠٢٥، ٥٦)، كما تشدد السياسات على حماية المعلومات في بيئات التعليم الإلكتروني من خلال التحقق من أمن الأنظمة التعليمية، وضمان جودة البث وتسجيل الجلسات، إلى جانب توجيه المجتمع الجامعي نحو الاستخدام المسؤول لوسائل التواصل الاجتماعي بما يحمي الخصوصية ويحافظ على السمعة الأكاديمية (جامعة عين شمس ، ١٨،٢٠٢٥).

وعلى مستوى الأنشطة المؤسسية، يبرز **المؤتمر السنوي العشرون لمركز تعليم الكبار** نموذجًا عمليًا لالتزام الجامعة بتعزيز الأمن السيبراني وحماية البيانات في السياق التعليمي، إذ يركز المؤتمر على التوعية بمخاطر الهجمات الإلكترونية وسرقة الهوية الرقمية، واستعراض أفضل الممارسات العالمية في حماية الخصوصية، فضلًا عن دعم محو الأمية الرقمية عبر برامج وورش عمل تهدف إلى تمكين المتعلمين من تأمين بياناتهم. كما يناقش المؤتمر دور التكنولوجيا والذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية، ويؤكد على تدريب الكوادر الأكاديمية لمواجهة هذه

التحديات وضمان استدامة الأمان الرقمي في بيئات التعليم والبحث (جامعة عين شمس ، ٢٠٢٥، https://www.asu.edu.eg/ar/825/event).

وبناءً على ما سبق، يتضح أن سياسات جامعة عين شمس في حماية البيانات والخصوصية تمثل إطارًا متكاملًا يعزز الثقة في البيئة البحثية الرقمية، ويجمع بين الابتكار التقني، والالتزام بالأطر الأخلاقية والقانونية، وتوفير بيئة رقمية آمنة، وبذلك، تساهم الجامعة في دعم الباحثين وتمكينهم من إنتاج معرفة علمية رصينة، بما يرسخ مكانتها كجامعة رائدة في تحقيق التحول الرقمي المستدام في مجال البحث العلمي والتعليم العالي.

القوى والعوامل الثقافية المؤثرة

تتأثر سياسات حماية البيانات والخصوصية في مصر بمجموعة من العوامل الثقافية والتكنولوجية والاقتصادية المتداخلة. فمن **الناحية الثقافية والاجتماعية**، تستند جامعة عين شمس إلى قانون حماية البيانات الشخصية لعام ٢٠٢٠، الذي لا يزال في طور التطوير مقارنة بالتشريعات الغربية، كما أن الوعي المجتمعي بالخصوصية الرقمية لم يصل بعد إلى المستوى المطلوب، مما يحد من فاعلية التطبيق العملي لهذه السياسات (حماية البيانات الشخصية، ٢٠٢٠, https://manshurat.org/node/66932)، ومع ذلك، تعمل الجامعة على تعزيز الوعي بأمن المعلومات في سياق التحول الرقمي، مع تركيز سياساتها على حماية السمعة المؤسسية وضبط استخدام البيانات بما يضمن النزاهة الأكاديمية، ويتجلى ذلك في **ميثاق السلوك الجامعي**.

وعلى الصعيد التكنولوجي، على الرغم من الجهود المبذولة لتأمين منصات التعلم الإلكتروني، تواجه الجامعة قيودًا مالية وتقنية تحد من تبني أنظمة أمنية متقدمة مماثلة لتلك المعمول بها في الجامعات الغربية، مما يجعل النهج التدريجي قائمًا على

تحسين البنية التحتية الرقمية وتعزيز القدرات في مجال الأمن السيبراني ضمن الإمكانات المتاحة. (Ain Shams University, 2023, https://www.asu.edu.eg/1014/page).

كما تعتمد الجامعة على أنظمة أكثر تقليدية، وتسعى لتقليص الفجوة التكنولوجية من خلال بناء شراكات بحثية دولية تهدف إلى رفع مستوى الأمان الرقمي وتعزيز قدراتها في حماية البيانات. ويعكس هذا الواقع أن العامل التكنولوجي لا يحدد فقط مستوى حماية البيانات، بل يؤثر أيضًا في قدرة المؤسسات الأكاديمية على التوازن بين متطلبات الأمن الرقمي والانفتاح العلمي.

خامسًا: التحليل المقارن

تشارك جامعة عين شمس وجامعة كاليفورنيا بيركلي في التزامهما الاستراتيجي بحماية البيانات والخصوصية وفق معايير صارمة تضمن سرية المعلومات والحفاظ علي النزاهة البحثية، ويبرز هذا الالتزام في اعتماد كلتا الجامعتين على سياسات واضحة وأدوات فعالة للحفاظ على أمن البيانات في مختلف مراحل البحث والنشر العلمي، بما يعزز ثقة الباحثين في بيئتهما الأكاديمية.

تتشابه الجامعتان في اعتمادهما على **أحدث تقنيات الأمن السيبراني**، بما في ذلك أساليب التشفير المتقدمة وأنظمة الحماية عالية الكفاءة، إلى جانب حرصهما على توفير برامج تدريبية مستمرة للباحثين وأعضاء هيئة التدريس في مجال الأمن الرقمي، ويسهم هذا النهج في تعزيز جاهزية الكوادر الأكاديمية والبحثية، وتمكينها من مواجهة التهديدات الإلكترونية بفعالية أكبر.

وفيما يتعلق **بالإطار القانوني والتنظيمي**، تلتزم جامعة كاليفورنيا بيركلي بالقوانين واللوائح الدولية مثل GDPR وHIPAA وFERPA، بينما ترتكز جامعة عين شمس

على السياسات المحلية المرتبطة بالأمن السيبراني مع مراعاة المعايير الدولية ذات الصلة، وعلى الرغم من اختلاف المرجعيات التشريعية، فإن الهدف المشترك يتمثل في ضمان حماية البيانات الأكاديمية والبحثية من أي انتهاكات.

كذلك، تولي الجامعتان أهمية خاصة **لحماية البيانات في مجال البحث الأكاديمي والنشر العلمي**، حيث تعتمدان على مستودعات بحثية موثوقة، وتؤكدان على ضرورة إزالة البيانات الوصفية قبل النشر، فضلًا عن ضمان نزاهة عملية مراجعة الأقران، ويعكس ذلك حرصهما على الجمع بين الانفتاح العلمي وحماية خصوصية المعلومات.

وأخيرًا، يتجسد التشابه بين الجامعتين في **تعزيز الوعي بالأمن السيبراني** عبر تنظيم مؤتمرات علمية متخصصة، وورش عمل، وبرامج تدريبية تهدف إلى رفع مستوى الوعي بالمخاطر الرقمية وتقديم أفضل الممارسات لحماية البيانات، ويساعد هذا التوجه على ترسيخ ثقافة أمنية مشتركة داخل المجتمع الأكاديمي تسهم في دعم الابتكار وضمان بيئة رقمية آمنة للبحث العلمي.

على الرغم من وجود بعض أوجه التشابه، تكشف المقارنة بين جامعة كاليفورنيا بيركلي وجامعة عين شمس عن **اختلافات جوهرية** في سياسات حماية البيانات والخصوصية، تعود بدرجة أساسية إلى تباين الظروف الاقتصادية والاجتماعية والسياسية والثقافية، بالإضافة إلى تفاوت مستويات التطور التكنولوجي بين الجامعتين. ويظهر هذا التباين بوضوح في طبيعة السياسات والإجراءات المتبعة؛ إذ تتأثر كل جامعة بهذه العوامل في رسم استراتيجياتها الخاصة بأمن المعلومات وحماية البيانات الأكاديمية والبحثية.

فمن الناحية الاقتصادية، يُعد التمويل أحد المحددات الرئيسة لمستوى الأمان الرقمي في المؤسسات الأكاديمية، إذ تمتلك جامعة كاليفورنيا بيركلي ميزانية بحثية

واسعة تُمكّنها من الاستثمار في بنية تحتية متطورة للأمن السيبراني، وتطبيق أنظمة حماية متقدمة، فضلًا عن تصميم برامج تدريبية متخصصة وتوظيف خبراء تقنيين على درجة عالية من الكفاءة لضمان حماية بيانات الطلاب والباحثين (University of California ,2023, www.berkeley.edu) ، وفي المقابل تواجه جامعة عين شمس تحديات مالية تحد من قدرتها على تبني أحدث تقنيات الحماية الرقمية، ما يدفعها إلى الاعتماد على بدائل منخفضة التكلفة مثل البرمجيات مفتوحة المصدر، إلى جانب تعزيز شراكاتها مع مؤسسات دولية لدعم تطوير بنيتها الرقمية (محمود فوزي أحمد، وعماد نجم عبدالحكيم، ٢٠١٨، ٣٩٥).

وفي هذا الإطار، تجسد بيركلي نموذجًا لمؤسسة أكاديمية تستند إلى موارد مالية واستثمارات استراتيجية ضخمة، مكّنتها من بناء منظومة متكاملة متوافقة مع تشريعات دولية صارمة مثل **GDPR** و**HIPAA** و**FERPA**، بما يعكس قدرتها على تطبيق سياسات متقدمة كـ"الخصوصية بحكم التصميم" و"الامتثال القانوني المسبق"، لضمان حماية البيانات في مختلف مراحل البحث والنشر الأكاديمي، أما جامعة عين شمس، فترتكز على نهج تدريجي في التحول الرقمي، تسعى من خلاله إلى استثمار مواردها المحدودة في تطوير البنية التحتية الأساسية وتعزيز الأمن السيبراني عبر التدريب ودعم البحث التطبيقي، في إطار بيئة اقتصادية أكثر تقييدًا.

وعلى **الصعيد السياسي**، يعكس توجه بيركلي اندماج الجامعات الأمريكية في منظومة تشريعية دولية متماسكة، حيث تشكل السياسات القانونية العالمية مرجعًا رئيسًا لإدارة البيانات وحماية الخصوصية، في المقابل، تعتمد عين شمس على الأطر الوطنية واللوائح الداخلية، وهو ما يعكس طبيعة النظام السياسي المصري الذي يمنح أولوية للأمن القومي والحفاظ على الهوية الرقمية، أكثر من الانفتاح على الأطر التشريعية الدولية.

كما يمكن تفسير التباين بين الجامعتين في ضوء الأطر المفاهيمية المرتبطة بالموضوع؛ إذ تُجسّد تجربة جامعة كاليفورنيا بيركلي مفهوم **الحوكمة الرقمية (Digital Governance)** الذي يقوم على صياغة سياسات تنظيمية متكاملة تُوازن بين متطلبات الانفتاح العلمي وضمان حماية الخصوصية، من خلال بنية تحتية متقدمة وتوظيف تقنيات حديثة لإدارة البيانات **(Marvin et al., 2023,** https://www.sciencedirect.com/science/article/pii/S0148296323001352)، وفي المقابل، تميل تجربة جامعة عين شمس إلى تبني منظور **الأمن الرقمي المؤسسي (Institutional Digital Security)** الذي يركز بالدرجة الأولى على حماية البنية التحتية التعليمية والبحثية من التهديدات السيبرانية، وهو توجه يعكس محددات سياقية ترتبط بواقع محدودية الموارد وإكراهات البيئة المحلية **(Md Alimul et al. ,2023,** https://rd.springer.com/article/10.1007/s42979-023-01984-x?utm)، وبهذا، يتضح أن بيركلي تتبنى نهجًا قائمًا على التكامل بين الانفتاح والضبط التنظيمي، بينما تركز عين شمس على البعد الوقائي لتعزيز استقرار منظومتها الرقمية.

يتضح أن الاختلافات بين سياسات حماية البيانات والخصوصية في جامعتي كاليفورنيا بيركلي وعين شمس تُعزى بدرجة كبيرة إلى اعتبارات اقتصادية وتكنولوجية وثقافية، فجامعة كاليفورنيا بيركلي، بما تمتلكه من موارد مالية واسعة وتقنيات متقدمة، قادرة على تبني سياسات صارمة وشاملة لحماية البيانات وضمان أمنها، في المقابل، تواجه جامعة عين شمس تحديات ترتبط بمحدودية التمويل والبنية التحتية الرقمية، غير أنها تعمل على توظيف استراتيجيات بديلة، مثل تعزيز التعاون الدولي والاعتماد على تقنيات منخفضة التكلفة، لدعم منظومة أمن المعلومات، وفي ضوء تزايد أهمية الأمان الرقمي في البيئات الأكاديمية، تظل الشفافية، والاستثمار في التطوير

المستمر، وتنمية الوعي الثقافي بعوامل الخصوصية الرقمية مرتكزات أساسية لتعزيز حماية البيانات وضمان استدامة الممارسات البحثية والتعليمية.

سادسًا: الآليات المقترحة لسياسات حماية البيانات والخصوصية في الجامعات المصرية على ضوء خبرة جامعة كاليفورنيا بيركلي

في **جامعة كاليفورنيا بيركلي**، تُعد سياسات **حماية البيانات والخصوصية** جزءًا أساسيًا من منظومة البحث الأكاديمي، حيث تعتمد الجامعة على معايير متقدمة لضمان أمن المعلومات والامتثال للتشريعات الدولية مثل **اللائحة العامة لحماية البيانات (GDPR) وقانون خصوصية المستهلك في كاليفورنيا (CCPA)**. تتبنى الجامعة تقنيات متطورة تشمل **التشفير، وإخفاء الهوية، وإدارة الوصول لحماية البيانات البحثية ومنع الاختراقات**، مع التركيز على التوعية والتدريب المستمر **لأعضاء هيئة التدريس والباحثين** والطلاب، كما تلتزم بوضع إجراءات استجابة فعالة للطوارئ للتعامل مع أي تهديدات محتملة للخصوصية، مما يعزز بيئة بحثية آمنة وموثوقة تُشجع على الابتكار والتعاون الأكاديمي مع الحفاظ على **سرية البيانات وحمايتها من الاستغلال غير المشروع.**

يمكن اقتراح مجموعة من الآليات لتعزيز سياسات حماية البيانات والخصوصية في الجامعات المصرية بما يسهم في تحسين الأداء البحثي. وتشمل هذه الآليات ما يلي:-

١. وضع إطار قانوني وتنظيمي واضح.

- تطوير سياسات مؤسسية شاملة لحماية البيانات والخصوصية وفقًا للمعايير الدولية.

- الالتزام بتشريعات حماية البيانات، مثل اللائحة العامة لحماية البيانات (GDPR)أو معايير مماثلة تتناسب مع البيئة القانونية المصرية.
- إنشاء وحدات متخصصة داخل الجامعات لمتابعة تنفيذ السياسات وضمان الامتثال لها.

٢. تعزيز البنية التحتية التقنية لحماية البيانات.

- تبني أنظمة تشفير متقدمة لحماية البيانات البحثية من الاختراقات أو الاستخدام غير المصرح به.
- تطبيق تقنيات إخفاء الهوية (Anonymization) وإدارة الوصول (Access Management)لضمان استخدام البيانات بشكل آمن.
- استخدام الحوسبة السحابية مع ضمان توافر تدابير الحماية والامتثال لمعايير الأمان.

٣. بناء ثقافة الوعي بالخصوصية والأمان السيبراني.

- تنظيم دورات تدريبية منتظمة لأعضاء هيئة التدريس والباحثين حول أخلاقيات البيانات وأفضل الممارسات في حماية الخصوصية.
- إدراج مادة دراسية ضمن مناهج الدراسات العليا حول أخلاقيات البحث العلمي وحماية البيانات.
- إطلاق حملات توعية دورية لتعريف الطلاب والباحثين بأهمية الأمن السيبراني وطرق حماية بياناتهم.

٤. تعزيز الشفافية في جمع البيانات واستخدامها.

- وضع سياسات واضحة لإدارة البيانات البحثية تشمل إجراءات جمع البيانات وتخزينها ومشاركتها مع الجهات الخارجية.

- توفير بوابات إلكترونية تتيح للباحثين التحكم في كيفية استخدام بياناتهم والجهات التي يمكنها الوصول إليها.
- إلزام الباحثين بتقديم خطة إدارة بيانات – (Data Management Plan DMP) عند التقدم بمشاريع بحثية.

٥. إنشاء مراكز متخصصة لأمن البيانات والبحث الأخلاقي.

- تأسيس مراكز لحوكمة البيانات تتولى مراجعة وضمان الامتثال لسياسات الخصوصية داخل الجامعات.
- تعزيز التعاون مع مراكز الأبحاث الدولية مثل جامعة كاليفورنيا بيركلي لتبادل الخبرات في مجال حماية البيانات البحثية.
- تطوير شراكات مع شركات الأمن السيبراني لتوفير حلول مبتكرة لحماية البيانات.

٦. دعم البحث العلمي القائم على البيانات المفتوحة **(Open Data)** مع ضمان الحماية.

- وضع سياسات تسمح بمشاركة البيانات البحثية بشكل مفتوح ولكن ضمن ضوابط تحمي خصوصية المشاركين.
- إنشاء مستودعات بيانات بحثية آمنة تتيح للباحثين مشاركة بياناتهم مع الحفاظ على حقوق الملكية الفكرية.
- تطبيق معايير FAIR (Findable, Accessible, Interoperable, Reusable) لضمان إدارة البيانات البحثية بكفاءة وأمان.

٧. تطوير آليات للاستجابة لحوادث الاختراق والتسرب المعلوماتي.

- إنشاء فرق استجابة لحوادث الأمن السيبراني داخل الجامعات للتعامل السريع مع أي اختراقات محتملة.
- وضع خطط طوارئ لمواجهة حوادث تسرب البيانات وتأمين استمرارية العمليات البحثية.
- التعاون مع الجهات المختصة لإنشاء قواعد بيانات مركزية لحماية المعلومات البحثية من الهجمات الإلكترونية.

الخلاصة

تُبرز تجربة جامعة كاليفورنيا بيركلي الدور المحوري الذي تؤديه السياسات الصارمة لحماية البيانات والخصوصية في تعزيز بيئة البحث العلمي وترسيخ الثقة بالمنظومة الأكاديمية. وفي ضوء ذلك، يصبح من الضروري للجامعات المصرية العمل على صياغة إطار قانوني متكامل ينظم هذا المجال، مدعومًا بتطوير البنية التحتية التقنية بما يواكب متطلبات البحث المعاصر. كما يستدعي الأمر تنمية ثقافة الوعي بالخصوصية لدى الباحثين وأعضاء هيئة التدريس، إلى جانب تشجيع الانخراط في الأبحاث المعتمدة على البيانات المفتوحة، مع ضمان توفير أعلى مستويات الأمان والحماية، بما يسهم في الارتقاء بجودة الإنتاج العلمي ودعم تنافسيته عالميًا.

المراجع

اولًا: المراجع العربية:-

١) على، عبير أحمد (٢٠٢٠). سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، **مجلة دراسات تربوية واجتماعية**, ٢٦(٣), ١٣٣-٢٠٠، متاح على

https://jsu.journals.ekb.eg/article_231281_94a108cd395c9b6961341672d7fc4116.pdf.

٢) أمين، مصطفى أحمد. (٢٠١٨). التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة. **مجلة الإدارة التربوية**، س٥, ع١٩ ، ١١ – ١١٦، ص٩٥. متاح علي http://search.mandumah.com/Record/1055494 .

٣) جمهورية مصر العربية رئاسة مجلس الوزراء المجلس الأعلى للأمن السيبراني (٢٠١٧). **الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)**، ص٥ ، متاح على https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf.

٤) يس، إيمان عبدالحميد، و السيد، أماني محمد. (٢٠٢٢). حماية البيانات الشخصية بالمكتبات الجامعية في مصر: دراسة استكشافية. **اعلم**، ع٣٢ ، ١٥٣ – ١٧٠. متاح على http://search.mandumah.com/Record/1379767.

٥) الامم المتحدة حقوق الانسان (٢٠٢٠). **بروتوكول بيركلي: إرشادات حول استخدام المعلومات الرقمية العامة للنضال من أجل حقوق الإنسان**، متاح على https://www.ohchr.org/ar/stories/2020/12/berkeley-protocol-gives-guidance-using-public-digital-info-fight-human-rights.

٦) جامعة عين شمس (٢٠٢٥). **مدونة الاخلاقيات الجامعية**، متاح علي https://www.asu.edu.eg/ar/862/page.

٧) جامعة عين شمس (٢٠٢٥). **المؤتمر السنوي العشرون لمركز تعليم الكبار بعين شمس بعنوان "الأمن السيبراني وتعليم الكبار في الوطن العربي"** ، متاح على https://www.asu.edu.eg/ar/825/event.

٨) محمود فوزي أحمد، وعماد نجم عبدالحكيم. (٢٠١٨). تعزيز تنافسية التعليم العالي المصري: مدخلا لتطوير واقع مؤسساته في تصنيفات نخبة الجامعات العالمية. **المجلة التربوية:** جامعة سوهاج – كلية التربية، ج٥٣ ، ٣٩٥.

٩) حماية البيانات الشخصية (٢٠٢٠) رقم ١٥١ لسنة ٢٠٢٠. **جمهورية مصر العربية**، متاح على https://manshurat.org/node/66932.

ثانيًا: المراجع الأجنبية:-

1. Ain Shams University (2023). **University Policies**, Available at https://www.asu.edu.eg/1014/page.
2. Ain Shams University (2025). **Cyber Security Program**, Available at https://chp-cis.asu.edu.eg/page/10#..
3. Berkeley Library (2025). **Peer review**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/publishing.
4. Berkeley Library (2025). **Publishers**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/publishing.
5. Berkeley Library (2025). **The lifecycle**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/publishing.
6. Berkeley Library (2025). AI, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
7. Berkeley Library (2025). **Copyright basics**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.

8. Berkeley Library (2025). **Dissertations**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
9. Berkeley Library (2025). **Fair use**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
10. Berkeley Library (2025). **Licensing**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
11. Berkeley Library (2025). **Managing copyright**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
12. Berkeley Library (2025). **Open access**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
13. Berkeley Library (2025). **Our program**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/about .
14. Berkeley Library (2025). **Publishing issues**, Available at https://www.lib.berkeley.edu/research/scholarly-communication/copyright.
15. Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in it: a review of techniques and challenges. **Computer Science & IT Research Journal**, 5(3), 606-615.
16. Faster Capita (2024).Confidentiality in research: **Maintaining Privacy in Scientific Studies**, Available at https://fastercapital.com/content/Confidentiality-in-research--Maintaining-Privacy-in-Scientific-Studies.html.
17. Regulation, P. (2018). General data protection regulation. **Intouch**, 25, 1-5**,** Available at https://www.into.ie/app/uploads/2019/10/GDPR_FAQ.pdf.
18. Hanisch, M., Goldsby, C. M., Fabian, N. E., & Oehmichen, J. (2023). Digital governance: A conceptual framework and research agenda. **Journal of Business Research**, 162, 113777,

Available at https://www.sciencedirect.com/science/article/pii/S0148296323001352.

19. Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in universities: An evaluation model. **SN Computer Science**, 4(5), 569, Available at https://rd.springer.com/article/10.1007/s42979-023-01984-x?utm .
20. IEP (2025). UC Berkeley Rated Number One Public University in the World and Fourth Best Overall by U.S. News, Available at https://iep.berkeley.edu/content/uc-berkeley-rated-number-one-public-university-world-and-fourth-best-overall-us-news.
21. Maltese, V. (2024). Addressing digital transformation in universities: How to effectively govern, trust and value institutional data. **Journal of Telecommunications and the Digital Economy**, 12(1), 242-260, Available at https://iris.unitn.it/bitstream/11572/406129/1/JTDE - Addressing digital transformation in universities preprint.pdf.
22. O'Toole, E., Feeney, L., Heard, K., & Naimpally, R. (2018). **Data security procedures for researchers. J-PAL North America**, Available at https://www.povertyactionlab.org/sites/default/files/data-security-procedures.pdf.
23. Smart, M. A., & Tan, D (2022). **Privacy and Security Challenges in Doctoral Students' Human Subjects Research**, Available at https://www.usenix.org/system/files/soups2022-poster31_smart_abstract_final.pdf.
24. Times Higher Education (2025). **University of California, Berkeley,** Available at https://www.timeshighereducation.com/world-university-rankings/university-california-berkeley.

25. University of California. (2023). **Privacy and Data Security Policies.** Retrieved from www.berkeley.edu.
26. UC Berkeley (2025). **Office of Ethics, Risk, and Compliance Services**, Available at https://oercs.berkeley.edu/about.