مجلة جامعة فزان العلمية
Fezzan University scientific Journal
journal@fezzanu.edu.ly

نحو إطار متكامل لحماية البيانات في عصر الذكاء الاصطناعي والبيانات الضخمة

*مصباح ابوبكر مصباح ابوبكر [1]
[1]قسم نظم المعلومات، كلية تقنية المعلومات، جامعة الجفرة

الملخص

يشهد العالم الرقمي تحديات متزايدة بفعل التطورات في الذكاء الاصطناعي والبيانات الضخمة، حيث أصبحت البيانات المورد الأكثر قيمة في الاقتصاد الرقمي وأساسًا لاتخاذ القرارات في مختلف القطاعات. ورغم وجود تشريعات مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR)، إلا أن المخاطر التقنية والقانونية والأخلاقية تتفاقم مع تعقيد الخوارزميات، وتوسع نطاق البيانات.

تتمثل التحديات التقنية في الهجمات السيبرانية المتطورة، وضعف آليات التشفير التقليدية، وإمكانية إعادة تحديد الهوية رغم تقنيات الإخفاء. أما التحديات القانونية فتشمل: قصور التشريعات الوطنية، والتباين بين الأطر الدولية، وضعف آليات التنفيذ، وهو ما يعيق التعاون العالمي. بينما التحديات الأخلاقية ترتبط باستخدام البيانات في المراقبة الجماعية، والتنبؤ بالسلوكيات، أو استغلالها تجاريًا دون موافقة صريحة، مما يهدد القيم الإنسانية الأساسية.

توضح دراسة حالة Cambridge Analytica – Facebook أن البيانات الشخصية يمكن أن تتحول إلى أداة قوة سياسية واقتصادية، وأن أي تسريب أو سوء استخدام قد يغير مسار دول بأكملها. ومن هنا، يقترح البحث إطارًا متكاملًا يجمع بين الحلول التقنية (مثل التشفير وإخفاء الهوية والحوسبة الآمنة متعددة الأطراف)، والحلول التنظيمية (سياسات الامتثال، آليات المراقبة، العقوبات)، والحلول الأخلاقية (الشفافية، إشراك المستخدمين).

يخلص البحث إلى أن حماية البيانات في عصر الذكاء الاصطناعي والبيانات الضخمة لا يمكن أن تتحقق إلا عبر تكامل الأبعاد التقنية والقانونية والأخلاقية، بما يضمن بيئة رقمية آمنة ومستدامة، ويعزز الثقة بين الأفراد والمؤسسات.

الكلمات المفتاحية: الأخلاقيات، البيانات الضخمة، الخصوصية، الذكاء الاصطناعي، التشريعات، حماية البيانات، الهجمات السيبرانية

Towards an Integrated Framework for Data Protection in the Age of Artificial Intelligence and Big Data

*Musbah Abobaker Musbah Abobaker[1]
[1]Department of Information Systems – Faculty of Information Technology – Aljufra University

Abstract

The digital era is witnessing unprecedented challenges due to the rapid growth of artificial intelligence (AI) and big data technologies. Data has become the most valuable resource in the digital economy, yet its misuse poses serious risks to privacy

*المؤلف الرئيسي: عناوين البريد الإلكتروني musbah.musbah@ju.edu.ly تاريخ استلام البحث 2 فبراير 2026 استلام رد المحكمين 23فبراير 2026 تم قبوله18 فبراير 2026 تاريخ النشر 26 مارس 2026

and security. Despite existing regulations such as the European General Data Protection Regulation (GDPR), technical, legal, and ethical gaps remain.
Technically, organizations face advanced cyberattacks, limitations of traditional encryption, and risks of re-identification despite anonymization methods. Legally, many national frameworks fail to keep pace with technological innovation, while inconsistencies between international regulations hinder global cooperation. Ethically, the use of data for mass surveillance, behavioral prediction, and commercial exploitation without explicit consent threatens fundamental human values.
The Cambridge Analytica–Facebook case illustrates how personal data can be weaponized for political and economic influence, undermining trust and prompting stricter regulations worldwide. To address these challenges, the paper proposes an integrated framework combining three dimensions: technical solutions (strong encryption, anonymization, secure multi-party computation), organizational measures (compliance policies, monitoring mechanisms, sanctions), and ethical practices (transparency, user participation, accountability.(
The study concludes that effective data protection in the age of AI and big data requires a holistic approach that unites technology, law, and ethics. Such integration ensures sustainable digital environments, strengthens institutional trust, and safeguards individual rights against misuse of personal information.
Keywords: Artificial Intelligence, Big Data, Cyberattacks, Data Protection, Ethics, Legislation, Privacy.

1. المقدمة

يشهد العالم الرقمي المعاصر ثورة غير مسبوقة بفعل التطورات المتسارعة في تقنيات الذكاء الاصطناعي (AI) والبيانات الضخمة(Big Data) ، حيث أصبحت البيانات المورد الأكثر قيمة في الاقتصاد الرقمي وأساسًا لاتخاذ القرارات في مختلف القطاعات الطبية، التعليمية، الصناعية، والأمنية. وكما يشير Hewage وآخرون "إن الابتكارات في الذكاء الاصطناعي والتعلم الآلي أحدثت تأثيرات واسعة على المجتمع والاقتصاد، لكنها في الوقت ذاته خلقت مخاطر جدية على حقوق الأفراد إذا لم يتم تطويرها والتحقق منها بشكل مسؤول "[1] . هذا الواقع يضع حماية البيانات في قلب النقاشات الأكاديمية والسياسات العامة، خاصة وأن انتهاكات الخصوصية أصبحت أكثر شيوعًا مع توسع استخدام تقنيات التحليل الخوارزمي، كما يؤكد palm وآخرون" البحوث الأكاديمية، مثلها مثل باقي المجالات، تتأثر بعمق بالتحديات التي يفرضها الذكاء الاصطناعي على حماية البيانات الشخصية "[2] .

رغم وجود تشريعات مثل اللائحة العامة لحماية البيانات الأوروبية (GDPR) ، إلا أن التحديات تتفاقم مع تعقيد تقنيات الذكاء الاصطناعي وتوسع نطاق البيانات الضخمة. وكما يوضح Taddeo و Floridi " تراكم البيانات الشخصية مع تطور أساليب التحليل، وإعادة الدمج يزيد من احتمالية تعرض البيانات الحساسة لانتهاكات، ويضع القانون أمام تحديات غير مسبوقة" [3].

يمكن تلخيص المشكلة البحثية في ثلاثة أبعاد رئيسية:

- التحديات التقنية :ضعف آليات التشفير أمام هجمات متقدمة، صعوبة ضمان الشفافية في خوارزميات الذكاء الاصطناعي، ومخاطر التحيز الخوارزمي.
- التحديات القانونية :قصور التشريعات في مواكبة الابتكارات التقنية، وتباين الأطر القانونية بين الدول مما يعيق التعاون الدولي.

- التحديات الأخلاقية :تتعلق باستخدام البيانات في المراقبة الجماعية، التنبؤ بالسلوكيات، أو استغلالها تجاريًا دون موافقة صريحة، مما يهدد القيم الإنسانية الأساسية.

يهدف هذا البحث إلى:

- تحليل الإطار النظري لحماية البيانات في ظل الذكاء الاصطناعي والبيانات الضخمة.
- تحديد الثغرات التقنية والقانونية والأخلاقية التي تواجه المؤسسات والأفراد.
- اقتراح إطار متكامل يجمع بين الحلول التقنية، التشريعية، والأخلاقية لتعزيز حماية البيانات.
- تقديم توصيات عملية لصناع القرار والباحثين حول السياسات المستقبلية.

وتتمثل أسئلة البحث الرئيسة في:

- كيف تؤثر تقنيات الذكاء الاصطناعي والبيانات الضخمة على خصوصية وأمن البيانات؟
- ما هي أبرز الثغرات القانونية في التشريعات الحالية لحماية البيانات؟
- كيف يمكن معالجة التحديات الأخلاقية المرتبطة باستخدام البيانات في التطبيقات الذكية؟
- ما ملامح الإطار المتكامل المقترح لحماية البيانات في العصر الرقمي؟

يعتمد البحث على منهجية مزدوجة:

- التحليل النظري :مراجعة الأدبيات الأكاديمية والتشريعات الدولية المتعلقة بحماية البيانات، مع التركيز على الدراسات الحديثة في مجال الذكاء الاصطناعي والبيانات الضخمة.
- دراسة تحليلية :تحليل حالات واقعية ودراسات حالة (Case Studies) حول انتهاكات البيانات أو نجاحات في تطبيق سياسات الحماية، بهدف استخلاص الدروس وتحديد أفضل الممارسات.
- اعتماد نهج النمذجة المفاهيمية المدمج مع تحليل الحالات التطبيقية. أولاً: يتم بناء إطار نظري يدمج الأبعاد التقنية والقانونية والأخلاقية لحماية البيانات استنادًا إلى مراجعة الأدبيات. ثانيًا: يتم تحويل هذا الإطار إلى نموذج كمي (IDPEM). ثالثًا: يتم تطبيق النموذج على حالة كامبريدج أناليتيكا–فيسبوك باستخدام تقديرات قائمة على السيناريوهات لإظهار قدرته التحليلية. وأخيرًا، يتم تحليل سيناريو السياسات المقارن (قبل وبعد البيئة التنظيمية) لتقييم حساسية النموذج.

2. الإطار النظري

2.1. تعريف حماية البيانات والخصوصية

تُعرّف حماية البيانات بأنها مجموعة من السياسات والتقنيات والإجراءات التي تهدف إلى ضمان سرية وسلامة وتوافر المعلومات الشخصية والبيانات الحساسة، ومنع الوصول غير المصرح به إليها أو استخدامها بشكل غير قانوني [4]. أما الخصوصية، فهي الحق الأساسي للفرد في التحكم بكيفية جمع بياناته واستخدامها ومشاركتها، وهو ما عبّر عنه Warrenو Brandeis منذ عام 1890 بمفهوم "الحق في أن يُترك المرء وشأنه" [6].

تطورت النظريات حول الخصوصية من اعتبارها مجرد مسألة تتعلق بالإفصاح عن المعلومات، إلى كونها عملية معقدة لتنظيم الحدود الشخصية والتحكم في تدفق المعلومات ضمن السياقات الاجتماعية والتقنية [10].

2.2. تطور المفاهيم عبر العقود

شهدت مفاهيم حماية البيانات والخصوصية تطورًا ملحوظًا عبر العقود:

الخمسينيات–السبعينيات :التركيز على حماية المعلومات في المؤسسات الحكومية والعسكرية، مع ظهور قوانين مثل Privacy Act of 1974 في الولايات المتحدة.(Information privacy, 2023)

الثمانينيات–التسعينيات : توسع الاهتمام ليشمل حماية البيانات الشخصية في المؤسسات التجارية، وظهور مصطلح Data Protection كحق قانوني في أوروبا.

الألفية الجديدة :الانتقال من حماية المعلومات إلى حماية الهوية الرقمية، حيث أصبحت الهوية الإلكترونية أساسًا للتعاملات الاقتصادية والاجتماعية.(Robles-Carrillo, 2024)

العقد الأخير : بروز تحديات الذكاء الاصطناعي والبيانات الضخمة، حيث لم تعد حماية البيانات مقتصرة على منع الوصول غير المصرح به، بل شملت ضمان الشفافية، العدالة، ومنع التحيز الخوارزمي [5].

2.3. أهم النظريات والمقاربات

أ. الأمن السيبراني

الأمن السيبراني يمثل المقاربة التقنية لحماية البيانات، ويشمل استراتيجيات التشفير، أنظمة كشف التسلل، وإدارة الهوية الرقمية. وكما يؤكد Christen وآخرون " :الأمن السيبراني لم يعد مجرد حماية للبنية التحتية، بل أصبح ضرورة لضمان الثقة في البيئة الرقمية" [6].

ب. أخلاقيات المعلومات

تتناول أخلاقيات المعلومات القضايا المتعلقة باستخدام البيانات بشكل مسؤول، مثل احترام الخصوصية، منع التمييز، وضمان العدالة في الوصول إلى المعلومات Narwal .وآخرون يشيرون إلى أن" التحديات الأخلاقية في حماية البيانات تتعلق بالحدود بين المصلحة العامة والحقوق الفردية، خاصة في ظل الاعتماد المتزايد على الذكاء الاصطناعي" [8].

ج. التشريعات الدولية

تشكل التشريعات الدولية الإطار القانوني لحماية البيانات، مثل اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، واتفاقيات الأمم المتحدة حول الحقوق الرقمية. يوضح Babikian أن" :القوانين الدولية تسعى إلى تحقيق توازن بين حرية تدفق البيانات عبر الحدود وحماية الخصوصية الفردية، لكنها تواجه تحديات في التطبيق العملي بسبب اختلاف السياقات الوطنية" [4] .

يُظهر هذا العرض أن حماية البيانات والخصوصية ليست مجرد قضية تقنية، بل هي منظومة متكاملة تشمل أبعادًا قانونية وأخلاقية واجتماعية. تطور المفاهيم من حماية المعلومات إلى حماية الهوية الرقمية يعكس التحولات العميقة في المجتمع الرقمي. كما أن النظريات والمقاربات المختلفة (الأمن السيبراني، أخلاقيات المعلومات، التشريعات الدولية) تشكل معًا أساسًا لفهم التحديات الراهنة واقتراح حلول متكاملة.

3. التحديات التقنية في حماية البيانات

3.1. الهجمات السيبرانية وأساليب الاختراق الحديثة

تُعد الهجمات السيبرانية من أبرز التحديات التقنية التي تواجه حماية البيانات في العصر الرقمي. فمع تطور أدوات الذكاء الاصطناعي، أصبحت أساليب الاختراق أكثر تعقيدًا ودقة. على سبيل المثال، يشير Alsmadi وZhang إلى أن "الهجمات السيبرانية لم تعد تعتمد على أساليب تقليدية مثل التصيد الإلكتروني، بل تطورت لتشمل هجمات مدعومة بالذكاء الاصطناعي قادرة على التكيف مع أنماط الدفاع " [11].

من أبرز الأساليب الحديثة:

1. هجمات الفدية (Ransomware) التي تستهدف المؤسسات الصحية والمالية، حيث يتم تشفير البيانات وطلب فدية مقابل فك التشفير.
2. الهجمات القائمة على الذكاء الاصطناعي مثل توليد رسائل تصيد مخصصة باستخدام تقنيات معالجة اللغة الطبيعية.
3. الهجمات على سلاسل التوريد الرقمية، والتي تستغل الثغرات في البرمجيات الموثوقة لنشر برمجيات خبيثة.

هذه التطورات تجعل من الصعب على المؤسسات مواكبة التهديدات، خاصة مع محدودية الموارد التقنية والبشرية في بعض القطاعات.

3.2. مخاطر البيانات الضخمة والذكاء الاصطناعي: إعادة تعريف التلاعب بالخوارزميات

البيانات الضخمة والذكاء الاصطناعي يفتحان آفاقًا واسعة للتحليل والتنبؤ، إلا أنهما في الوقت ذاته يخلقان مخاطر جديدة. كما يوضح Zuboff أن " الاقتصاد القائم على المراقبة يعيد تعريف العلاقة بين الأفراد والمؤسسات، حيث تصبح البيانات أداة للتلاعب بالسلوكيات البشرية عبر الخوارزميات) " [14].

من أبرز المخاطر:

- إعادة تعريف التلاعب بالخوارزميات :حيث يمكن استخدام الذكاء الاصطناعي لتوجيه قرارات الأفراد بشكل غير مباشر عبر توصيات مخصصة أو محتوى مُفلتر.
- التحيز الخوارزمي :إذ قد تؤدي البيانات غير المتوازنة إلى نتائج غير عادلة، مثل التمييز في التوظيف أو الخدمات المالية.
- المراقبة الجماعية :استخدام البيانات الضخمة في تتبع الأنشطة الرقمية للأفراد، مما يهدد الخصوصية والحقوق الأساسية.

يشيران Palmو Lindblom إلى أن " التحديات الأخلاقية والقانونية المرتبطة بالذكاء الاصطناعي لا تنفصل عن التحديات التقنية، إذ أن الخوارزميات نفسها قد تصبح أداة لانتهاك الخصوصية) " [2].

3.3. أدوات الحماية التقنية

لمواجهة هذه التحديات، طُورت مجموعة من الأدوات التقنية التي تهدف إلى تعزيز حماية البيانات:

أ. التشفير (Encryption)

يُعد التشفير من أقدم وأكثر الأدوات فعالية في حماية البيانات. وفقًا لـ Stallings " التشفير يمثل خط الدفاع الأول ضد الوصول غير المصرح به، لكنه يواجه تحديات في الأداء والقدرة على التوسع مع البيانات الضخمة) " [13].

ب. إخفاء الهوية(Anonymization)

إخفاء الهوية يهدف إلى إزالة أو تعديل البيانات الشخصية بحيث لا يمكن ربطها مباشرة بالفرد. ومع ذلك، يشير Narwal وآخرون إلى أن" :إعادة تحديد الهوية ممكنة في كثير من الحالات عبر تقنيات الدمج والتحليل، مما يقلل من فعالية إخفاء الهوية التقليدي) " [12].

ج. الحوسبة الآمنة متعددة الأطراف(Secure Multi-Party Computation)

تُعد هذه التقنية من الابتكارات الحديثة، حيث تسمح لأطراف متعددة بإجراء عمليات حسابية على بيانات مشتركة دون الكشف عن البيانات نفسها. Christen .وآخرون يؤكدون أن" الحوسبة الآمنة متعددة الأطراف توفر توازنًا بين الخصوصية وإمكانية التعاون، لكنها ما تزال تواجه تحديات في الأداء العملي" [6].

تُظهر هذه المراجعة أن التحديات التقنية في حماية البيانات ليست مجرد مسألة أمنية، بل هي منظومة معقدة تشمل الهجمات السيبرانية المتطورة، المخاطر الناجمة عن البيانات الضخمة والذكاء الاصطناعي، وأدوات الحماية التقنية التي تحتاج إلى تطوير مستمر. إن مواجهة هذه التحديات تتطلب تكاملًا بين الحلول التقنية، القانونية، والأخلاقية لضمان حماية فعالة ومستدامة للبيانات في العصر الرقمي.

جدول (1): الأبعاد الثلاثة للإطار المتكامل لحماية البيانات

البعد	التحديات الرئيسة	الحلول المقترحة
البعد التقني	–الهجمات السيبرانية المتطورة –ضعف التشفير التقليدي –مخاطر إعادة تحديد الهوية	–التشفير القوي –إخفاء الهوية المتقدم –الحوسبة الآمنة متعددة الأطراف
البعد القانوني	–قصور التشريعات الوطنية –التباين بين الأطر الدولية –ضعف آليات التنفيذ	–سن قوانين متخصصة –مواءمة التشريعات مع المعايير الدولية –إنشاء هيئات مستقلة للرقابة
البعد الأخلاقي	–المراقبة الجماعية –التنبؤ بالسلوكيات –الاستغلال التجاري دون موافقة	–تعزيز الشفافية –إشراك المستخدمين في القرارات –الالتزام بالمساءلة والمسؤولية الاجتماعية

4. الأبعاد القانونية والأخلاقية لحماية البيانات

4.1. قانون الخصوصية القانونية

تُعد الخصوصية حقًا أساسيًا من حقوق الإنسان، وقد تم تكريسه في العديد من المواثيق الدولية مثل الإعلان العالمي لحقوق الإنسان (المادة 12) والعهد الدولي للحقوق المدنية والسياسية (المادة 17). يشير Taddeo و Floridi إلى أن "القانون يواجه تحديًا غير مسبوق في مواكبة التطورات التقنية، حيث لم تعد حماية البيانات مجرد مسألة تنظيمية، بل أصبحت جزءًا من حماية الكرامة الإنسانية) " [3].

القوانين الوطنية غالبًا ما تركز على حماية البيانات الشخصية من الاستخدام غير المشروع، لكنها تختلف في نطاقها وفعاليتها. على سبيل المثال، في الولايات المتحدة يركز قانون الخصوصية على حماية المستهلك، بينما في أوروبا يُعتبر الحق في حماية البيانات جزءًا من الحقوق الأساسية.

4.2. التجارب العربية

شهدت المنطقة العربية تطورات متفاوتة في مجال حماية البيانات:

المغرب وتونس :أصدرتا قوانين لحماية البيانات الشخصية مستوحاة من النموذج الأوروبي، مع إنشاء هيئات وطنية للإشراف على تطبيق هذه القوانين.

الإمارات العربية المتحدة :أطلقت قانون حماية البيانات في عام 2021 كجزء من استراتيجيتها للتحول الرقمي.

ليبيا :رغم وجود إشارات إلى حماية الخصوصية في بعض التشريعات، إلا أن الإطار القانوني المتكامل لحماية البيانات لم يتبلور بشكل واضح حتى الآن. تشير بعض الدراسات إلى أن" التجربة الليبية ما تزال في طور التأسيس، وتعتمد بشكل كبير على التشريعات العامة المتعلقة بالاتصالات والمعلوماتية دون وجود قانون متخصص لحماية البيانات" [15].

4.3. التشريعات الدولية: اللائحة الأوروبية والتجربة الليبية

تُعتبر اللائحة العامة لحماية البيانات الأوروبية (GDPR) الصادرة عام 2018 النموذج الأكثر شمولًا في حماية البيانات عالميًا. فهي تفرض التزامات صارمة على المؤسسات فيما يتعلق بجمع البيانات ومعالجتها، وتمنح الأفراد حقوقًا موسعة مثل الحق في النسيان والحق في نقل البيانات [16].

في المقابل، تفتقر ليبيا إلى إطار قانوني مماثل، مما يخلق فجوة كبيرة بين التشريعات المحلية والدولية. هذه الفجوة تؤثر على قدرة المؤسسات الليبية على التعاون الدولي، خاصة في المجالات التي تتطلب تبادل البيانات عبر الحدود مثل التعليم والبحث الطبي.

4.4. الفجوات بين التشريعات المحلية والدولية

الفجوة بين التشريعات المحلية والدولية تتجلى في عدة نقاط:

- غياب التشريعات المتخصصة في بعض الدول العربية؛ مما يجعل حماية البيانات مقتصرة على نصوص عامة.
- ضعف آليات التنفيذ، حيث لا توجد هيئات مستقلة قادرة على مراقبة تطبيق القوانين.
- تباين المعايير، إذ تختلف متطلبات حماية البيانات بين الدول، مما يعيق التعاون الدولي.

كما يشير Hewage وآخرونإلى أن " التباين بين الأطر القانونية الوطنية والدولية يخلق بيئة غير مستقرة، ويضع المؤسسات أمام تحديات في الامتثال للقوانين المتعددة والمتناقضة أحيانًا" [1].

4.5. التوازن بين الابتكار وحماية الخصوصية

أحد أبرز التحديات يتمثل في إيجاد توازن بين الابتكار التقني وحماية الخصوصية. فالذكاء الاصطناعي والبيانات الضخمة يوفران فرصًا هائلة في مجالات مثل الصحة والتعليم، لكنهما يثيران مخاطر جدية على الخصوصية.

يصف Zuboff هذا الوضع بأنه "اقتصاد المراقبة الذي يحول البيانات إلى سلعة، ويعيد تعريف العلاقة بين الأفراد والمؤسسات) " [14]. ومن هنا، يصبح التحدي هو كيفية الاستفادة من الابتكار دون التضحية بحقوق الأفراد الأساسية.

4.6. المسؤولية الأخلاقية للمؤسسات والشركات

لا تقتصر حماية البيانات على الجانب القانوني فقط، بل تشمل أيضًا المسؤولية الأخلاقية للمؤسسات والشركات. فالمؤسسات مطالبة بتبني سياسات شفافة في جمع البيانات واستخدامها، وضمان عدم استغلالها لأغراض غير مشروعة.

" الأخلاقيات في مجال حماية البيانات ليست مجرد التزام قانوني، بل هي شرط أساسي لبناء الثقة بين المؤسسات والمجتمع" [6] .

المسؤولية الأخلاقية تشمل:

- احترام خصوصية الأفراد.
- ضمان العدالة وعدم التمييز في استخدام البيانات.
- الالتزام بمبادئ الشفافية والمساءلة.

تُظهر هذه المراجعة أن الأبعاد القانونية والأخلاقية لحماية البيانات تشكل أساسًا لفهم التحديات الراهنة. فالقوانين الوطنية والدولية تسعى إلى حماية الخصوصية، لكن الفجوات بينهما تخلق تحديات إضافية. كما أن التوازن بين الابتكار وحماية الخصوصية يتطلب مقاربة شاملة تجمع بين القانون والأخلاق والتقنية. وفي النهاية، فإن المسؤولية الأخلاقية للمؤسسات والشركات هي الضمان الحقيقي لبناء بيئة رقمية آمنة ومستدامة.

5. دراسة حالة: فضيحة " Cambridge Analytica – Facebook "

5.1. خلفية الواقعة

- في عام 2013، طوّر الباحث ألكسندر كوغان تطبيقًا باسم This Is Your Digital Life عبر منصة فيسبوك.
- التطبيق جمع بيانات المستخدمين الذين حمّلوه، لكنه أيضًا استخرج بيانات أصدقائهم عبر واجهة Open Graph الخاصة بفيسبوك.
- هذه البيانات وصلت إلى شركة الاستشارات السياسية البريطانية Cambridge Analytica، التي استخدمتها في بناء ملفات نفسية دقيقة للملايين.

5.2. حجم التسريب

- تم الوصول إلى بيانات حوالي 87 مليون مستخدم حول العالم.
- تضمنت البيانات: الاهتمامات، الإعجابات، العلاقات الاجتماعية، والمعلومات الشخصية.
- لم يكن هناك موافقة صريحة من المستخدمين على هذا الاستخدام.

5.3. الأهداف والاستخدامات

- الهدف الأساسي كان التأثير على السلوك الانتخابي عبر الإعلانات الموجهة.(Micro-targeting)
- استخدمت Cambridge Analytica البيانات في حملات مثل :
  - الانتخابات الرئاسية الأمريكية 2016.
  - استفتاء خروج بريطانيا من الاتحاد الأوروبي.(Brexit)

5.4. الانتهاكات الأخلاقية والقانونية

- غياب الموافقة :لم يُخطر المستخدمون بأن بياناتهم ستُستخدم لأغراض سياسية.
- انتهاك الخصوصية :استغلال ثغرات في واجهة فيسبوك لجمع بيانات الأصدقاء.
- غياب الشفافية :لم يكن هناك وضوح حول كيفية جمع البيانات أو استخدامها.
- تضليل المستخدمين :تم التلاعب بالرأي العام عبر محتوى موجه بناءً على نقاط ضعف نفسية.

5.5. التداعيات والنتائج

- تراجع ثقة المستخدمين في فيسبوك بشكل كبير.
- استدعاء مارك زوكربيرغ للشهادة أمام الكونغرس الأمريكي والبرلمان الأوروبي.
- فرض غرامات ضخمة على فيسبوك، منها غرامة 5مليارات دولار من لجنة التجارة الفيدرالية.(FTC)
- دفع الحكومات والشركات إلى تعزيز قوانين حماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا.

5.6. الدروس المستفادة

- ضرورة الموافقة الصريحة قبل جمع أو استخدام البيانات.
- الشفافية في سياسات الخصوصية.
- المساءلة القانونية للشركات التي تتعامل مع بيانات المستخدمين.
- تعزيز الوعي الرقمي لدى الأفراد حول كيفية حماية بياناتهم.

جدول (2) مقارنة مختصرة مع تسريبات أخرى

الواقعة	حجم البيانات	الهدف	التداعيات
Cambridge Analytica – Facebook	87مليون مستخدم	التأثير السياسي	غرامات، فقدان الثقة، تشديد القوانين
اختراق–Yahoo (2013 2014)	3مليارات حساب	سرقة بيانات شخصية	انهيار سمعة الشركة، خسائر مالية
تسريب(2017) Equifax	147مليون شخص	بيانات مالية	دعاوى قضائية، غرامات بمئات الملايين

تُظهر هذه الواقعة والجدول(2) أن البيانات الشخصية ليست مجرد معلومات تقنية، بل أداة قوة سياسية واقتصادية .أي تسريب أو سوء استخدام يمكن أن يغيّر مسار دول بأكملها.

6. الإطار المقترح لمعالجة تسريبات البيانات الكبرى

المخطط بالشكل رقم(1) يوضح تداخل الأبعاد الثلاثة (تقني – تنظيمي – أخلاقي) في شكل دوائر متقاطعة (Venn Diagram)، مع إبراز المنطقة المشتركة كمنظومة متكاملة لحماية البيانات ومنع التسريبات الكبرى.

الشكل (1) المخطط البصري للإطار المقترح لمعالجة تسريبات البيانات

- الدائرة الزرقاء (تقني) : تمثل أدوات الحماية مثل التشفير وإخفاء الهوية.
- الدائرة الخضراء (تنظيمي) : تمثل السياسات والرقابة والعقوبات.
- الدائرة البرتقالية (أخلاقي): تمثل الشفافية وإشراك المستخدمين.
- المنطقة الوسطى المتقاطعة : تمثل الحماية الشاملة التي لا تتحقق إلا بتكامل الأبعاد الثلاثة.

أولًا: الحلول التقنية

- التشفير :(Encryption)
  - اعتماد تقنيات تشفير قوية مثلًا AES–256 لحماية البيانات أثناء النقل والتخزين.

- تطبيق التشفير الطرفي (End-to-End) لضمان أن البيانات لا تُقرأ إلا من قبل المرسل والمستقبل.

- إخفاء الهوية:(Anonymization)
  - إزالة أو تشويش المعرفات الشخصية (مثل الأسماء، البريد الإلكتروني، رقم الهاتف.
  - استخدام تقنيات التفاضل الخصوصي (Differential Privacy) لتقليل إمكانية إعادة التعرف على الأفراد.
- الحوسبة الآمنة متعددة الأطراف:(Secure Multi-Party Computation)
  - تمكين عدة أطراف من إجراء عمليات حسابية على البيانات المشتركة دون كشف البيانات لبعضهم البعض.
  - مفيد في حالات التعاون بين مؤسسات مختلفة مع الحفاظ على سرية البيانات.

ثانيًا: الحلول التنظيمية

- سياسات الامتثال:(Compliance Policies)
  - إلزام المؤسسات بتطبيق معايير مثل GDPR في أوروبا أو CCPA في كاليفورنيا.
  - وضع سياسات واضحة لإدارة دورة حياة البيانات (جمع، تخزين، مشاركة، حذف).
- آليات المراقبة:(Monitoring Mechanisms)
  - إنشاء وحدات مستقلة لمراجعة وضبط ممارسات البيانات داخل المؤسسات.
  - استخدام أدوات تدقيق دورية لكشف أي خروقات أو سوء استخدام.
- العقوبات:(Sanctions)
  - فرض غرامات مالية ضخمة على المؤسسات المخالفة (كما حدث مع فيسبوك – 5 مليارات دولار)
  - تقييد الأنشطة التجارية أو تعليق التراخيص في حال تكرار الانتهاكات.

ثالثًا: الحلول الأخلاقية

- تعزيز الشفافية:(Transparency)
  - نشر تقارير دورية توضح كيفية جمع البيانات واستخدامها.
  - توفير لوحات تحكم للمستخدمين لرؤية وإدارة بياناتهم.
- إشراك المستخدمين في قرارات البيانات:(User Participation)
  - منح المستخدمين حق الموافقة أو الرفض قبل مشاركة بياناتهم مع أطراف ثالثة.
  - تفعيل خيارات "الانسحاب (Opt-out) "بسهولة ووضوح.
  - إشراك المستخدمين في صياغة سياسات الخصوصية عبر استطلاعات أو لجان استشارية.

الجمع بين الحلول التقنية (لحماية البيانات فعليًا)، والحلول التنظيمية (لضمان الامتثال والمساءلة)، والحلول الأخلاقية (لإعادة بناء الثقة مع المستخدمين) يُشكّل منظومة متكاملة قادرة على تقليل مخاطر التسريبات المستقبلية، وتحويل إدارة البيانات من مجرد التزام قانوني إلى ممارسة مسؤولة ومستدامة.

الجدول (3) يوضح الإطار المقترح بالامثلة العملية ليعطي فهم أوسع للقارئ .

جدول (3) مقارن للإطار المقترح لمعالجة تسريبات البيانات الكبرى

البُعد	الحلول المقترحة	أمثلة تطبيقية عملية	الأثر المتوقع
تقني	-التشفير القوي(AES-256، End-to-End). -إخفاء الهوية عبر التفاضل الخصوصي. -الحوسبة الآمنة متعددة الأطراف.	-تطبيق واتساب يستخدم التشفير الطرفي. -جوجل تطبق تقنيات التفاضل الخصوصي في إحصاءات الاستخدام. -تعاون البنوك عبر بروتوكولات الحوسبة الآمنة دون كشف بيانات العملاء.	-تقليل فرص الاختراق. -حماية هوية المستخدمين. -تمكين التعاون الآمن بين المؤسسات.
تنظيمي	-سياسات الامتثال(GDPR ، CCPA). -آليات المراقبة والتدقيق الدوري. -العقوبات والغرامات.	-غرامة 5 مليارات دولار على فيسبوك من لجنة التجارة الفيدرالية. -إنشاء وحدات مستقلة لمراجعة البيانات داخل المؤسسات. -إلزام الشركات بتقارير سنوية عن الخصوصية.	-تعزيز الالتزام القانوني. -ردع الانتهاكات. -رفع مستوى الثقة المؤسسية.
أخلاقي	-تعزيز الشفافية عبر تقارير دورية. -إشراك المستخدمين في قرارات البيانات. -توفير خيارات الانسحاب (Opt-out).	-لوحات تحكم الخصوصية في فيسبوك وجوجل. -استطلاعات رأي المستخدمين حول سياسات البيانات. -إشراك المجتمع المدني في صياغة السياسات.	-بناء الثقة مع المستخدمين. -تمكين الأفراد من التحكم في بياناتهم. -تقليل الفجوة بين الشركات والجمهور.

هذا الجدول يُظهر أن الحلول التقنية وحدها لا تكفي، بل يجب أن تُدمج مع إطار تنظيمي صارم وممارسات أخلاقية شفافة لضمان حماية البيانات ومنع تكرار فضائح مثل .Cambridge Analytica.

6.1. تشكيل الإطار المقترح في نموذج IDPEM

تقوم هذه الدراسة بتحويل الإطار المفاهيمي إلى نموذج علمي رسمي يُسمى نموذج الفعالية المتكاملة لحماية البيانات . (IDPEM)يفترض النموذج أن فعالية حماية البيانات (DPE) هي دالة موزونة لثلاثة أبعاد أساسية: الحماية التقنية (T)، الامتثال القانوني(L) ، والحوكمة الأخلاقية (E) ,ويُعبر عن النموذج بالصيغة التالية:

$$DPE=\alpha T+\beta L+\gamma E$$

حيث :

- DPE = فعالية حماية البيانات .
- T = مؤشر الحماية التقنية .
- L = مؤشر الامتثال القانوني.
- E = مؤشر الحوكمة الأخلاقية .
- $\alpha+\beta+\gamma=1$

في حالة غياب المعايرة التجريبية، يُفترض أن الأوزان متساوية كخط أساس محايد لعرض النموذج.

حيث تعكس الأوزان التأثير النسبي لكل بُعد، وتُحقق الشرط $DPE=\alpha T+\beta L+\gamma E$. ويتم تفكيك كل بُعد إلى مؤشرات قابلة للقياس، مما يتيح التقييم التجريبي والتحليل المقارن عبر المؤسسات والسياقات الوطنية.

6.1.1. المؤشرات الفرعية

كل متغير رئيسي هو بدوره مكوّن من عناصر فرعية:

أولا : المؤشر التقني T

$$T = \frac{1}{n}\sum_{i=1}^{n} t_i$$

حيث t_i يمثل عناصر مثل :

العنصر	(t_i)
قوة التشفير	t_1
أنظمة كشف التسلل	t_2
إدارة الهوية	t_3
مقاومة إعادة التعريف	t_4
أمن البنية السحابية	t_5

ثانيا : المؤشر القانوني :-

$$L = \frac{1}{m}\sum_{j=1}^{m} l_j$$

حيث l_j يمثل عناصر مثل :

العنصر	(l_j)
وجود قانون حماية بيانات	l_1
هيئة رقابية مستقلة	l_2
آلية العقوبات	l_3
حقوق الأفراد	l_4
الامتثال الدولي	l_5

ثالثا : المؤشر الأخلاقي E:-

$$E = \frac{1}{k}\sum_{k=1}^{k} k_e$$

حيث k_e يمثل عناصر مثل :

العنصر	(k_i)
الشفافية	k_1
الموافقة الصريحة	k_2
المساءلة	k_3
عدم التمييز الخوارزمي	k_4
اشراك المستخدمين	k_5

وكما ذكرت سابقا فان النظام يعتمد كليا على قيمة الأبعاد حيث ينهار النظام إذا انهار أحد الأبعاد؛ أى أنه هناك شرطا، وهو : (dependency principle) If $T<T_{min}$ or $I<I_{min}$ or $e<e_{min}$ => DPE => Low

وبما أن الأوزان $\alpha+\beta+\gamma=1$ وبما أن تمثيل الأوزان من 0.0 الى 0.9 فإن قيم الانحدار التاثيري يبدء بأقل من 0.5 وصولا الى 0.0

الجدول (4) يوضح مثالا تطبيقيا على ذلك

الحالة	T	L	E	النتيجة
شركة تكنولوجية بدون قانون	0.8	0.2	0.6	حماية ضعيفة
دولة لديها قانون دون تقنية	0.3	0.9	0.7	حماية غير فعالة
نظام متوازن	0.8	0.8	0.8	حماية قوية

6.1.2. تطبيق النموذج (IDPEM)على دراسة الحالة

نتذكر أن النموذج هو $DPE=T\alpha+L\beta+E\gamma$ حيث $\frac{1}{3}=\gamma=\beta=\alpha$

تقييم المؤشر التقني T:

العنصر	التقييم	السبب
قوة التشفير	0.7	فيسبوك لديه بنية أمنية قوية
إدارة الهوية	0.5	ضوابط الوصول للتطبيق كانت ضعيفة
حماية API	0.2	سمح بسحب بيانات الأصدقاء
منع إعادة الاستخدام	0.3	لا يوجد رقابة على استخدام البيانات من طرف ثالث
المراقبة الأمنية	0.4	لم يكتشف سوء الاستخدام المبكر

$$T=\frac{0.7+0.5+0.2+0.3+0.4}{5}=0.42$$

تقييم المؤشر القانوني L :

عنصر	التقييم	السبب
قانون حماية بيانات قوي	0.4	الحادثة قبل تشديدGDPR
الرقابة الحكومية	0.3	ضعف الرقابة على المنصات آنذاك
العقوبات الرادعة	0.6	الغرامات جاءت بعد الفضيحة
حقوق المستخدمين	0.4	لم يكن هناك وعي بحقوق البيانات
الامتثال الدولي	0.5	فيسبوك شركة عابرة للحدود لكن بدون التزام صارم

$$L = \frac{0.4 + 0.3 + 0.6 + 0.4 + 0.5}{5} = 0.44$$

تقييم المؤشر الأخلاقي E :

عنصر	التقييم	السبب
الشفافية	0.2	المستخدمون لم يعلموا بالاستخدام السياسي
الموافقة الصريحة	0.1	لا توجد موافقة حقيقية
المساءلة المؤسسية	0.3	الإنكار في البداية
عدم التلاعب	0.0	استهداف نفسي مباشر
إشراك المستخدمين	0.1	لا توجد سيطرة للمستخدم

$$\boldsymbol{E} = \frac{0.2 + 0.1 + 0.3 + 0.0 + 0.1}{5} = 0.14$$

حساب فعالية الحماية DPE :

$$\mathrm{DPE} = \frac{1}{3}(0.42) + \frac{1}{3}(0.44) + \frac{1}{3}(0.14)$$

$$\mathrm{DPE} = 0.14 + 0.15 + 0.05 = 0.34$$

$$\mathrm{DPE} = 0.34$$

يؤدي تطبيق نموذج IDPEM على حالة Cambridge Analytica–Facebook إلى الحصول على قيمة لفعالية حماية البيانات (DPE) قدرها 0.34، مما يشير إلى بيئة حماية ضعيفة للغاية. ففي حين أظهرت الأبعاد التقنية (T=0.42) والقانونية (L=0.44) مستويات متوسطة، انهار مؤشر الحوكمة الأخلاقية (E=0.14)، وهو ما يوضح أن الفشل الأخلاقي يمكن أن يقوّض فعالية حماية البيانات بشكل عام حتى في ظل وجود بنى تحتية تقنية.

6.1.3. تطبيق النموذج (IDPEM) بعد تشديد القوانين "" افتراض واقعي ""

البعد	القيمة	الوضع
T	0.42	حماية تقنية متوسطة مع ثغرات API
L	0.44	تشريعات غير صارمة
E	0.14	انهيار أخلاقي
DPE	0.34	حماية ضعيفة

تذكير بالسيناريو القديم :

العنصر	التقييم
قوة التشفير	0.7
إدارة الهوية	0.8
حماية API	0.7
منع إعادة الاستخدام	0.6
المراقبة الأمنية	0.7

تقييم المؤشر التقني T:

$$T = \frac{0.7 + 0.8 + 0.7 + 0.6 + 0.7}{5} = 0.7$$

تقييم المؤشر القانوني L :

عنصر	التقييم
قانون حماية بيانات قوي	0.9
الرقابة الحكومية	0.8
العقوبات الرادعة	0.9
حقوق المستخدمين	0.9
الامتثال الدولي	0.8

$$\boldsymbol{L} = \frac{0.9 + 0.8 + 0.9 + 0.9 + 0.8}{5} = 0.86$$

تقييم المؤشر الأخلاقي E :

عنصر	التقييم
الشفافية	0.7
الموافقة الصريحة	0.8
المساءلة المؤسسية	0.7
عدم التلاعب	0.6
إشراك المستخدمين	0.7

$$E = \frac{0.7 + 0.8 + 0.7 + 0.6 + 0.7}{5} = 0.7$$

حساب فعالية الحماية DPE :

$$\mathrm{DPE} = \frac{1}{3}(0.7) + \frac{1}{3}(0.86) + \frac{1}{3}(0.7)$$

$$DPE = 0.23 + 0.28 + 0.23 = 0.74$$

$$DPE = 0.74$$

مما يعني أن فعالية الحماية قد تحسّنت بنسبة تقارب 120% تقريبا والسبب هو ارتفاع البعد القانوني والأخلاقي .

بعد إجراء تحليل مقارن باستخدام نموذج IDPEM يُظهر أن هناك تحسنًا كبيرًا في فعالية حماية البيانات عقب تعزيز الأطر التنظيمية. إذ ترتفع قيمة فعالية حماية البيانات (DPE) من 0.34 في سيناريو ما قبل التنظيم إلى 0.75 في بيئة ما بعد تطبيق اللائحة العامة لحماية البيانات (GDPR). ويؤكد ذلك أن آليات الحوكمة التنظيمية والأخلاقية تسهم بشكل كبير في تعزيز الحماية الشاملة، بل وبدرجة تفوق أثر التحسينات التقنية وحدها.

"تعتمد القيم المستخدمة في تطبيق نموذج IDPEM على تقديرات قائمة على السيناريو(Scenario–based Estimates)، تم اشتقاقها من تحليل نوعي للأدبيات ودراسة الحالة (Cambridge Analytica–Facebook). وتهدف هذه القيم إلى توضيح الإطار التحليلي للنموذج وإبراز سلوكه التفسيري، دون الادعاء بأنها تمثل قياسات تجريبية دقيقة. ويُوصى في الدراسات المستقبلية بالتحقق التجريبي من هذه القيم باستخدام بيانات واقعية وأساليب إحصائية."

7. الخاتمة

تؤكد هذه الدراسة أن حماية البيانات في بيئة الذكاء الاصطناعي والبيانات الضخمة لم تعد مسألة تقنية بحتة، بل تمثل منظومة متعددة الأبعاد تتطلب تكاملًا بنيويًا بين الحماية التقنية، والامتثال القانوني، والحوكمة الأخلاقية. وانطلاقًا من هذا التصور، لم تكتفِ الدراسة بالطرح النظري، بل تضمن تحويل الإطار المفاهيمي إلى نموذج علمي رسمي هو نموذج الفعالية المتكاملة لحماية البيانات(IDPEM) ، الذي يعرّف فعالية الحماية بوصفها دالة موزونة تعتمد على الأبعاد الثلاثة المذكورة.

وقد أظهر التطبيق العملي للنموذج على حالة Cambridge Analytica–Facebook أن فعالية حماية البيانات بلغت (0.34)، وهي قيمة تعكس بيئة حماية ضعيفة، رغم وجود بنية تقنية وقانونية جزئية، نتيجة الانهيار الواضح في بعد الحوكمة الأخلاقية. ويكشف ذلك أن الفشل الأخلاقي يمكن أن يقوّض منظومة الحماية بالكامل حتى في وجود بنى تقنية متقدمة. كما بيّن التحليل المقارن للسيناريو التنظيمي اللاحق (بيئة ما بعد (GDPR) ارتفاع قيمة الفعالية إلى (0.75)، مما يبرهن على أن التعزيز التنظيمي والأخلاقي يسهمان بصورة حاسمة في رفع مستوى الحماية الشاملة، وبدرجة تفوق أثر التحسينات التقنية وحدها.

وعليه، فإن الإسهام العلمي لهذه الدراسة يتمثل في تقديم نموذج تحليلي قابل للقياس والمقارنة، يتيح تقييم فعالية أنظمة حماية البيانات على المستوى المؤسسي والوطني، ويمكّن صانعي السياسات والباحثين من فهم العلاقات التفاعلية بين الأبعاد التقنية والقانونية والأخلاقية بدل النظر إليها بصورة منفصلة. كما يفتح النموذج المجال أمام دراسات مستقبلية لتطوير أدوات قياس معيارية، وتطبيقات تجريبية أوسع في سياقات دولية مختلفة.

إن بناء بيئة رقمية آمنة ومستدامة يتطلب انتقالًا من المعالجات الجزئية إلى النماذج المتكاملة، حيث تُعد الحوكمة الأخلاقية عنصرًا حاسمًا في استدامة الثقة الرقمية، وليس مجرد بعد مكمل. ومن ثمّ، فإن أي استراتيجية وطنية أو مؤسسية لحماية البيانات ينبغي أن تُبنى على هذا التكامل البنيوي لضمان فاعلية حقيقية في مواجهة مخاطر العصر الرقمي.

يمثل نموذج IDPEM خطوة نحو تحويل حماية البيانات من إطار نظري إلى أداة تحليلية قابلة للقياس، ما يجعله أساسًا علميًا يمكن البناء عليه في الدراسات المستقبلية ووضع السياسات الرقمية.

اتجاهات البحث المستقبلية

يمكن للدراسات المستقبلية توسيع نموذج الفعالية المتكاملة لحماية البيانات (IDPEM) في عدة اتجاهات مهمة. أولًا: يُعد التحقق التجريبي من النموذج باستخدام بيانات واقعية على مستوى المؤسسات خطوة ضرورية لتعزيز موثوقيته الكمية، ولإتاحة المعايرة الإحصائية لأوزان المتغيرات (γ ، β، α). ثانيًا: يمكن تطوير مقاييس معيارية لكل مؤشر فرعي ضمن الأبعاد التقنية والقانونية والأخلاقية، بما يسهم في رفع مستوى الموضوعية. ثالثًا: من الممكن تكييف النموذج ليتناسب مع قطاعات محددة مثل الرعاية الصحية، والتقنيات المالية، والمدن الذكية، حيث تختلف حساسية البيانات والسياقات التنظيمية بشكل ملحوظ. إضافةً إلى ذلك، فإن دمج العوامل الديناميكية مثل تطور مخاطر الذكاء الاصطناعي، وشفافية القرارات المؤتمتة، والمساءلة الخوارزمية قد يعزز ملاءمة النموذج للبيئات الرقمية سريعة التغير. وأخيرًا، يمكن توظيف أساليب المحاكاة أو تقنيات التعلم الآلي للتنبؤ بكيفية تأثير التدخلات التنظيمية أو التقنية في فعالية حماية البيانات عبر الزمن.

8. قائمة المراجع

[1] C. Hewage, et al., *"Innovations in AI and machine learning: Impacts and risks,"* Journal of Information Security, 2023.

[2] E. Palm and J. Lindblom, *"Academic research and challenges of AI in data protection,"* Data & Ethics Review, 2022.

[3] M. Taddeo and L. Floridi, *"The ethics of data accumulation and re-identification,"* Philosophy & Technology, vol. 31, no. 4, pp. 1–15, 2021.

[4] G. Babikian, *"International data protection laws and challenges,"* International Law Review, 2020.

[5] D. Robles-Carrillo, *"Digital identity and data protection,"* Cyber Law Journal, 2024.

[6] M. Christen, et al*., "Cybersecurity and trust in digital environments,"* Information Ethics Journal, 2022.

[7] R. Narwal, et al., *"Ethical boundaries in AI-driven data use,"* AI & Society, vol. 35, no. 2, pp. 123–135, 2021.

[8] S. Warren and L. Brandeis, *"The right to privacy,"* Harvard Law Review, vol. 4, pp. 193–220, 1890.

[9] *"Privacy Act of 1974,"* United States Code, Public Law 93-579, Dec. 31, 1974.

[10] S. Schiffner, S. Ziegler, and M. Jensen, Privacy Symposium 2023: *"Data Protection Law International Convergence and Compliance with Innovative Technologies (DPLICIT) ",* Springer Nature, 2023.

[11] I. Alsmadi and J. Zhang, *"AI-powered cyberattacks: Emerging threats,"* Computers & Security, vol. 108, 2021.

[12] R. Narwal, et al., *"Re-identification risks in anonymization,"* AI & Society, 2021.

[13] W. Stallings, *"Cryptography and Network Security",* 8th ed., Pearson, 2020.

[14] S. Zuboff, *"The Age of Surveillance Capitalism*", PublicAffairs, 2019.

[15] DLA Piper, "*Data Protection Laws of the World: Libya*", Jan. 18, 2024.

[16] European Union, *"General Data Protection Regulation (GDPR),"* Regulation (EU) 2016/679, Apr. 27, 2016.