التنظيم القانوني للتخزين السحابي:
"دراسة مقارنة بين القانون الأوروبي والكويتي والمصري"

The legal regulation of cloud storage: A comparative study between European, Kuwaiti, and Egyptian law.

إعداد

المحامي د/ بدر سعد العتيبي

محامي محكمة التمييز والمحكمة الدستورية

وعضو في جمعية المحامين الكويتية

Prepared by Lawyer Dr. Badr Saad Al-Otaibi

Lawyer at the Court of Cassation and the Constitutional Court, and a member of the Kuwaiti Lawyers Association.

التنظيم القانوني للتخزين السحابي:
"دراسة مقارنة بين القانون الأوروبي والكويتي والمصري"

الملخص:

تتناول الدراسة موضوع التخزين السحابي من منظور قانوني وتقني. فتستعرض الدراسة مفهوم التخزين السحابي، وتسلط الضوء على الأبعاد التقنية والقانونية، والتطور التاريخي لتشريعات التخزين السحابي.

وتناولت الدراسة التنظيم القانوني في الاتحاد الأوروبي من خلال "اللائحة العامة لحماية البيانات (GDPR)"، التي تُعتبر نموذجًا متقدمًا في حماية البيانات الشخصية، وضمان أمنها. كما استعرضت الدراسة القوانين الحالية في كلًا من الكويت ومصر، وسلطت الدراسة الضوء على أوجه القصور التشريعية والتحديات الرئيسية التي تواجه تنظيم خدمات التخزين السحابي، مثل سيادة البيانات ونقلها عبر الحدود.

ومن خلال المقارنة بين الأطر القانونية الثلاثة، تبين وجود فروقات في مستوى الحماية والتنظيم بينهم، مما يستدعي تبني استراتيجيات قانونية موحدة لتعزيز الأمان والخصوصية في التخزين السحابي، مع تقديم توصيات لتطوير قوانين تتماشى مع الاطر الدولية، مع مراعاة الفوارق الاقتصادية والاجتماعية لكل من الكويت ومصر. وتوصلت الدراسة إلى أهمية التعاون بين الحكومات والكيانات الخاصة، لتعزيز الأمن السيبراني، وتحديث التشريعات لضمان حماية البيانات في عصر التحول الرقمي.

الكلمات المفتاحية: بنية التخزين - الأمن السيبراني - اللائحة العامة لحماية البيانات – الخصوصية.

Abstract:

The study addresses the topic of cloud storage from both legal and technical perspectives. It explores the concept of cloud storage, highlighting its technical and legal dimensions, along with the historical evolution of related legislation.

The study addresses the topic of cloud storage from a legal and technical perspective. It reviews the concept of cloud storage, highlighting the technical and legal dimensions, and the historical development of cloud storage legislation. The study examines the legal regulation in the "European Union through the General Data Protection Regulation (GDPR)", which is considered an advanced model in personal data protection and security assurance. It also reviews the current laws in both Kuwait and Egypt, shedding light on legislative shortcomings and the main challenges facing the regulation of cloud storage services, such as data sovereignty and cross-border data transfer.

Through a comparison of the three legal frameworks, the study reveals differences in the level of protection and regulation among them, calling for the adoption of unified legal strategies to enhance security and privacy in cloud storage. It provides recommendations for developing laws in line with international

frameworks, considering the economic and social differences in Kuwait and Egypt. The study concludes that collaboration between governments and private entities is crucial to enhancing cybersecurity and updating legislation to ensure data protection in the digital transformation era.

Keywords: Storage Infrastructure - Cybersecurity - General Data Protection Regulation - Privacy.

المقدمة

تقنيات التخزين السحابي من أهم الابتكارات التي غيّرت طريقة إدارة البيانات والمعلومات على مستوى الأفراد والشركات. فقد أتاحت هذه التقنية التعامل مع البيانات من أي مكان وفي الوقت الذي يرغب به المستخدم، مما ساعد في الكفاءة والمرونة في الوصل إليها. كما ساعدت هذه التقنية من تخزين كميات هائلة من البيانات والوصول إليها عبر الإنترنت بدلًا من الاعتماد على تخزين البيانات على أجهزة محلية. ومع ذلك، فإن استخدام التخزين السحابي يطرح العديد من التحديات المتعلقة بحماية البيانات، والمسؤولية عن الأضرار الناجمة عن الانتهاكات الأمنية أو الفشل في تقديم الخدمة.

فالقوانين التي تنظمه تعتبر من العناصر الأساسية، وذلك لضمان حماية البيانات وحقوق المستخدمين. وتتفاوت الأطر القانونية في الدول في تنظيم التخزين السحابي، يثير العديد من التساؤلات حول فعالية هذه الأطر في مواجهة التحديات القانونية والتقنية. وفي هذه الدراسة، نهدف إلى تحليل التنظيم القانوني للتخزين السحابي من خلال مقارنة التشريعات في كل من الاتحاد الأوروبي، والكويت، ومصر. إذ يُعتبر التشريع الأوروبي من أكثر الأطر تطورًا في الحفاظ على البيانات وحمايتها وذلك من خلال "اللائحة العامة لحماية البيانات (GDPR)"، بينما تُظهر القوانين في كلًا من الكويت ومصر اختلافات ملحوظة في المعايير والممارسات.

ستتناول الدراسة الاطر القانونية المختلفة المعنية بتخزين البيانات السحابي، بما في ذلك حقوق المستخدمين، وواجبات مزودي الخدمة، والعقبات التي تواجهها. ومن خلال التحليل للفروق والتشابهات بين القوانين، نسعى إلى تقديم حول لتحسين الأطر القانونية في الدول العربية، وذلك لمواكبة التطورات المتسارعة في مجال المعلومات.

ففهم التنظيم القانوني للتخزين السحابي ليس شأن أكاديمي وحسب، فهو ضرورة حيوية لضمان الحقوق في العصر الرقمي. ومن خلال هذه الدراسة، نأمل أن يتم تسليط الضوء على أفضل الممارسات القانونية، وتعزيز الحوار حول تطوير سياسات فعالة تعزز من الأمان والموثوقية في استخدام التخزين السحابي، مما يساعد على تقديم توصيات لتطوير التشريعات، وتحقيق التوازن الفعال بين الابتكارات، وحماية الحقوق.

هدف الدراسة:

تهدف الدراسة إلى تحليل وتقييم الأطر القانونية، المنظمة لخدمات التخزين السحابي، وذلك في ثلاث بيئات قانونية مختلفة، من خلال مقارنة الأطر التشريعية في الاتحاد الأوروبي مع نظيراتها في الكويت ومصر. وتسعى الدراسة إلى:

١- **تحليل الأطر القانونية**: دراسة القوانين والتشريعات المتعلقة بالتخزين السحابي في كل من الاتحاد الأوروبي، وكويت، ومصر، وكيفية تنظيم هذه التقنية.

٢- **تقييم الفعالية القانونية لحماية البيانات**: تقييم فعالية الأطر القانونية في حماية البيانات الخاصة، وحقوق المستخدمين في بيئة التخزين السحابي، مع التركيز على جوانب مثل الخصوصية، والأمان، والمسؤولية القانونية لمزودي الخدمة.

٣- **تحديد أوجه التشابه والاختلاف**: إبراز نقاط الالتقاء والاختلاف بين الأطر القانونية الأوروبية والعربية، فيما يتعلق بتنظيم تخزين البيانات في السحابة الالكترونية، مع التركيز على كفاءة تشريعيات، وحوكمة البيانات.

٤- **تقديم توصيات قانونية**: تقديم توصيات مستندة إلى النتائج المستخلصة من الدراسة، يمكن تطبيقها في الواقع العملي.

٥- **تعزيز الوعي القانوني**: تعزيز الوعي بين المستخدمين والشركات، حول الحقوق والواجبات في استخدام خدمات التخزين السحابي، مما يسهم في استخدام هذه التقنية بشكل آمن وموثوق.

فمن خلال تحقيق هذه الأهداف، تهدف الدراسة إلى تقديم رؤى شاملة تسهم في فهم التنظيم القانوني للتخزين السحابي، يمك تقديم توصيات مستندة إلى النتائج المستخلصة من الدراسة، يمكن تطبيقها في الواقع العملي.

أهمية الدراسة:

تأتي أهمية هذه الدراسة من الحاجة الملحة لفهم الأطر القانونية المستخدمة في التحكم في التخزين السحابي، وذلك في ظل التطورات التكنولوجية المتسارعة. فالبيانات تقوم بدورٍ محوريٍ في العالم الرقمي، ويُعد التخزين السحابي وسيلة رئيسية وسهلة لإدارة هذه البيانات بشكل فعال وآمن. ولذا فإن أهمية الدراسة تكمن في:

١- **تعزيز حماية البيانات:** تسعى هذه الدراسة إلى استكشاف القوانين حماية البيانات في الاتحاد الأوروبي، والكويت، ومصر، وتحديد مدى فعاليتها في حماية الحقوق، مع ضمان سرية المعلومات الشخصية المخزنة.

٢- **دعم الابتكار التكنولوجي:** الفهم العميق للأطر القانونية يمكن أن يسهم في تعزيز الابتكار، وذلك من خلال تشجيع الشركات والمطورين على استخدام التخزين السحابي بطرق تحفظ لهم حقوقهم.

٣- **تعزيز الثقة الرقمية:** فمن خلال تحليل القوانين، يمكن تقديم توصيات لتحسين البيئة الرقمية، وتعزيز الثقة بين الاطراف، مما ينعكس بالإيجاب على الاقتصاد الرقمي، ويشجع على تبني التكنولوجيا بشكل أوسع.

٤- **حماية حقوق الأفراد:** تهدف الدراسة إلى ضمان أن تكون القوانين والتشريعات قادرة على حماية الحقوق، كالخصوصية وحقوق الوصول إلى البيانات، مما يعزز الشعور بالأمان لدى المستخدمين.

٥- **التأثير العالمي** من خلال دراسة مقارنة بين قوانين مناطق مختلفة، يمكن تقديم نظرة شاملة عن تعامل النظم القانونية مع التكنولوجيا الحديثة عبر الثقافات والقوانين المختلفة. وهذا يساهم في وضع معايير دولية معنية بحماية البيانات.

ولذا تُعتبر هذه الدراسة خطوة مهمة نحو فهم التحديات والفرص المتعلقة بالتنظيم القانوني للتخزين السحابي، وتقديم رؤى وتوصيات تساعد في تطوير أطر قانونية تلبي احتياجات العصر الرقمي، وتحمي حقوق الأفراد، وتدعم الابتكارات. وذلك للوصول إلى فهم أعمق وأكثر شمولية لمعرفة التعامل مع التخزين السحابي في مختلف البيئات القانونية.

مشكلة الدراسة:

أن تتباين القوانين بين الدول، يثير العديد من التساؤلات حول حماية البيانات الخاصة، وحقوق المستخدمين. وبالتالي؛ يمكن تلخيص المشكلة في النقاط التالية:

١- **غياب التشريعات الموحدة:** تعاني الدول العربية، مثل الكويت ومصر، من نقص واضح في القوانين المتخصصة، والتي تنظم التخزين السحابي، مما يؤدي إلى ثغرات، قد تعرض البيانات الشخصية، والمؤسسية للخطر. وفي المقابل، يملك الاتحاد الأوروبي تشريع متقدم متمثل في "اللائحة العامة لحماية البيانات (GDPR)".

٢- **حماية البيانات والخصوصية:** يطرح استخدام التخزين السحابي أسئلة قانونية حول كيفية حماية البيانات، وضمان الخصوصية، خاصةً مع انتقال البيانات عبر الحدود

إلى خوادم دولية، مما يجعلها عرضة لانتهاكات قد تكون خارج نطاق القوانين المحلية.

٣- **المسؤولية:** عدم وضوح المسؤولية في حالة حدوث اختراقات أو فقدان للبيانات، سواء من جانب مزودي الخدمات السحابية أو المستخدمين، يُعد تحديًا قانونيًا كبيرًا.

٤- **التفاوت بين القوانين:** التفاوت الكبير بين القوانين الأوروبية، والقوانين الكويتية والمصرية يؤدي إلى اشكاليات في تطبيق المعايير العالمية، مما يؤثر على قدرة الدول العربية على مواكبة تلك المعايير.

٥- **التحديات التقنية والأخلاقية:** مع تزايد استخدام التخزين السحابي، تثار قضايا أخلاقية وقانونية جديدة تتعلق بكيفية معالجة البيانات، مما يتطلب تطوير أطر قادرة على التعامل مع هذه التحديات.

تمثل مشكلة الدراسة تحديًا معقدًا يتطلب تحليلًا دقيقًا للأطر القانونية الحالية والمقارنة بينها. ومن خلال تناول هذه المشكلة، تهدف الدراسة إلى تقديم رؤى وحلول قانونية فعالة تعزز من تنظيم التخزين السحابي وحماية حقوق المستخدمين.

اشكالية الدراسة:

مع التنامي في استخدام التخزين السحابي كوسيلة أساسية لحفظ البيانات وإدارتها، تبرز العديد من الإشكاليات. إذ يمثل التخزين السحابي تحديًا قانونيًا خاصًا نظرًا لطبيعته التقنية المعقدة والعابرة للحدود، فمعرفة مدى كفاية الأطر القانونية الحالية في حماية البيانات وتنظيم العلاقة بين المستخدمين ومزودي الخدمة، يمثل تساؤلًا هامًا.

فالإشكالية الرئيسية للدراسة تتمثل في؛ كيفية صياغة إطار قانوني شامل ينظم التخزين السحابي، يضمن حماية البيانات، وحقوق المستخدمين، ويواكب التطورات، مع مراعاة التفاوت بين الأطر القانونية المتقدمة في الاتحاد الأوروبي ونظيراتها في الدول العربية مثل الكويت ومصر.

أبعاد الإشكالية:

١- حماية البيانات والخصوصية:

- هل توفر التشريعات الكويتية والمصرية الضمانات الكافية، وذلك لحماية البيانات مقارنة "باللائحة العامة لحماية البيانات (GDPR)"؟
- كيف يمكن التعامل مع نقل البيانات عبر الحدود، والتي تخضع لقوانين دولية مختلفة؟

٢- تحديد المسؤولية القانونية:

- من هو الذي يتحمل المسؤولية، في حالة حدوث اختراقات أو فقدان للبيانات؟
- هل تُوفر العقود بين المستخدمين ومزودي الخدمة السحابية حماية قانونية كافية؟

٣- التفاوت بين القوانين المحلية والدولية:

- كيف يمكن للدول العربية، مثل الكويت ومصر، مواءمة تشريعاتها مع الأطر القانونية العالمية، خاصة تلك المطبقة في الاتحاد الأوروبي؟
- ما هي الثغرات التي تعيق استخدام التخزين السحابي بشكل آمن وفعال؟

٤- التحديات التقنية والقانونية:

- كيف يمكن صياغة قوانين مرنة وقابلة للتحديث لمواكبة التطور السريع في تقنيات التخزين السحابي؟

وبهذا تسعى الدراسة إلى تقديم حلول عملية للإشكاليات، وخاصة القانونية منها، التي تواجه التخزين السحابي، مع مقارنة الأطر القانونية بين الاتحاد الأوروبي والكويت ومصر.

تساؤلات الدراسة:

تركز هذه الدراسة على تحليل التنظيم القانوني للتخزين السحابي من خلال مقارنة الأطر في الاتحاد الأوروبي، الكويت، ومصر. ومن هنا، تسعى للإجابة عن:

التساؤل الرئيسي:

- كيف يمكن تنظيم التخزين السحابي بشكل قانوني، وذلك لضمان حماية البيانات وحقوق المستخدمين، مع الأخذ بعين الاعتبار الفروقات بين الأطر القانونية في الدول محل الدراسة؟

التساؤلات الفرعية:

١- التشريعات القائمة:

- ما هي أبرز القوانين المنظمة للتخزين السحابي في الدول محل الدراسة "الاتحاد الأوروبي، الكويت، ومصر"؟
- كيف تتعامل كل من هذه القوانين مع حماية البيانات الخاصة، والخصوصية؟

٢- حماية البيانات والخصوصية:

- ما مدى كفاءة القوانين الكويتية، والمصرية في حماية بيانات المستخدمين المحفوظة في السحابة؟
- كيف تختلف حماية البيانات بين "اللائحة العامة لحماية البيانات (GDPR)"، والتشريعات في الكويت ومصر؟

٣- المسؤولية القانونية:

- من يتحمل المسؤولية في حالة فقدان البيانات أو اختراقها في كل من هذه النظم القانونية؟
- كيف تُعالج العقود القانونية بين المستخدمين ومزودي خدمات التخزين السحابي في كل من الدول محل الدراسة؟

٤- التحديات التنظيمية:

- ما هي التحديات التي تواجهها كلًا من الكويت ومصر، لتطوير قانونيين متقدمة تتماشى مع المعايير الدولية؟
- كيف يمكن للدول العربية مواجهة تحديات نقل البيانات عبر الحدود الدولية؟

٥- التوافق مع المعايير الدولية:

- كيف يمكن مواءمة تشريعات كلًا من مصر والكويت، مع التشريعات الأوروبية المتقدمة مثل GDPR؟
- ما الدروس المستفادة من النموذج الأوروبي لتطوير قوانين محلية لتنظيم التخزين السحابي؟

وهذه التساؤلات تساعد في توجيه الدراسة نحو فهم شامل للإشكاليات المتعلقة بالتخزين السحابي، كما تُساهم في تقديم مقترحات عملية لتطوير التشريعات في الكويت ومصر.

فرضيات الدراسة:

تركز الدراسة على التنظيم القانوني للتخزين السحابي من خلال مقارنة الأطر التشريعية في الاتحاد الأوروبي، الكويت، ومصر. وبناءً على الإشكالية والتساؤلات المطروحة، تعتمد الدراسة التالي:

الفرضية الأولى: تُعد القوانين الأوروبية، مثل "اللائحة العامة لحماية البيانات (GDPR)"، أكثر شمولًا وكفاءة، في حماية البيانات والخصوصية، مقارنةً بالقوانين الكويتية والمصرية.

الفرضية الثانية: غياب قانون موحد لتنظيم التخزين السحابي، فيكلًا من الكويت ومصر، يؤدي إلى زيادة أخطار اختراق البيانات، وضعف الثقة التقنيات السحابية.

الفرضية الثالثة: المسؤولية القانونية عن أضرار الناجمة عن استخدام التخزين السحابي غير واضحة في التشريعات الكويتية والمصرية، مقارنةً بالأطر الأوروبية التي تحدد بوضوح مسؤوليات مزودي الخدمة والمستخدمين.

توفر هذه الفرضيات إطارًا استقصائيًا للقضايا القانونية المرتبطة بالتخزين السحابي، وتسهم في تحليل أوجه القصور في التشريعات الكويتية والمصرية، مع تقديم مقترحات مستنيرة لتحسينها بما يتماشى مع المعايير العالمية.

متغيرات الدراسة:

تتناول الدراسة التنظيم القانوني للتخزين السحابي من خلال دراسة التشريعات المقارنة في القانون الأوروبي والكويتي والمصري مجموعة من المتغيرات التي يمكن أن تؤثر على الموضوع. ويمكن تصنيف المتغيرات إلى نوعين رئيسيين: المتغيرات المستقلة والمتغيرات التابعة.

١- المتغيرات المستقلة

- **الإطار القانوني**: يشمل القوانين المعمول بها في الاتحاد الأوروبي، والكويت، ومصر، والمتعلقة بالتخزين السحابي.
- **معايير حماية البيانات الشخصية**: تتعلق بالمعايير المتبعة في كل نظام قانوني لحماية البيانات الخاصة، مثل "اللائحة العامة لحماية البيانات (GDPR)".
- **مسؤوليات مزودي الخدمة**: تتعلق بالالتزامات المفروضة على مزودي خدمات التخزين السحابي، وكيفية تعاملهم مع البيانات والانتهاكات.
- **الوعي القانوني**: يتضمن مدى معرفة الأفراد والشركات بحقوقهم وواجباتهم القانونية في استخدام خدمات التخزين السحابي.
- **التحديات التقنية**: تشمل الابتكارات، والتحديات المرتبطة بأمان البيانات وكفاءة التخزين السحابي.

٢- المتغيرات التابعة:

- **الثقة في خدمات التخزين السحابي**: مستوى الثقة الذي يشعر به المستخدمون تجاه مزودي خدمات التخزين السحابي بناءً على الأطر القانونية.

- **الامتثال القانوني**: مدى قدرة الأفراد والشركات على الامتثال للقوانين المتعلقة بالتخزين السحابي وحماية البيانات.
- **تأثير الانتهاكات القانونية**: كيفية تأثير الانتهاكات المحتملة للبيانات على الأفراد والشركات، وكذلك على سمعة مزودي الخدمة.

وهذه المتغيرات يمكن أن في فهم وتحليل العلاقة بين التنظيم القانوني للتخزين السحابي، والحقوق، والواجبات المرتبطة به. ومن خلال تحليل هذه المتغيرات، تسعى الدراسة إلى تقديم رؤى واضحة حول حماية البيانات في بيئة التخزين السحابي.

منهجية الدراسة:

تقوم منهجية الدراسة متعددة وتشمل المنهج الوصفي، المنهج التحليلي، والمنهج المقارن. وتكامل هذه المناهج يساعد على تقديم رؤية شاملة عن التنظيم القانوني للتخزين السحابي، مع تحليل التشريعات القائمة ومقارنتها بين الدول محل الدراسة.

١- **المنهج الوصفي:** يستند هذا المنهج إلى جمع البيانات، والمعلومات الخاصة بالقوانين، التي تحكم التخزين السحابي في كل من الاتحاد الأوروبي، والكويت، ومصر. وذلك لوصف الأطر التشريعية القائمة، وتحليل النصوص القانونية، بالإضافة إلى دراسة الممارسات التطبيقية المتعلقة بحماية البيانات الشخصية وإدارة التخزين السحابي في هذه المناطق.

٢- **المنهج التحليلي**: يستند هذا المنهج إلى تحليل القوانين والمعلومات التي تم جمعها باستخدام المنهج الوصفي. حيث يتم تحليلها لمعرفة مدى فعاليتها في حماية البيانات الخاصة وتحديد النقاط القوية والضعف في كل نظام قانوني.

٣- **المنهج المقارن:** يستند هذا المنهج لمقارنة الأطر القانونية للتخزين السحابي في الاتحاد الأوروبي، والكويت، ومصر. وهذا المنهج يساعد في تحديد الفروقات والتشابهات بين الأطر القانونية وتقديم توصيات لتحسينها.

تُمكّن هذه المنهجية المتكاملة الدراسة من تقديم تحليل شامل ومقارنة دقيقة للتنظيم القانوني للتخزين السحابي، مما يسهم في اقتراح أطر قانونية مُحكمة.

خطة الدراسة:

يتعرض الباحث لموضوع الدراسة من خلال إلقاء نظرة على مفهوم التخزين السحابي، والأبعاد التقنية والقانونية للتخزين السحابي، والتطور التاريخي للتشريعات المرتبطة بالتخزين السحابي. ثم يتم تناول التنظيم القانوني للتخزين السحابي في الاتحاد الأوروبي، وأثرة على حماية البيانات، ثم يتم تناول التنظيم القانوني للتخزين السحابي في الكويت ومصر. ومن ثم يتم مقارنة بين التشريعات الثلاث. وذلك؛ للوصول لمقترح إطار قانوني متكامل لتنظيم التخزين السحابي في كلًا من الكويت ومصر.

توفر هذه الخطة إطارًا متكاملًا لدراسة التنظيم القانوني للتخزين السحابي، مع تحليل الجوانب التقنية والقانونية ومقارنة التشريعات المختلفة لتقديم توصيات عملية وفعّالة.

مفهوم التخزين السحابي:

لقد ظهر التخزين السحابي كأحد الابتكارات البارزة التي غيرت طريقة تعاملنا مع البيانات والمعلومات الرقمية[(١)]، فالتخزين السحابي يتمحور حول تخزين البيانات عبر

(١) مفهوم الحوسبة كخدمة ليس جديدًا. حتى قبل ظهور مراكز البيانات الخاصة بالشركات، كانت الحوسبة تُقدم كخدمة عبر أجهزة الحاسوب الرئيسية التي تديرها الشركات الكبرى والوكالات الحكومية. وهذه الأجهزة كانت مكلفة وتحتاج إلى موارد كبيرة لإدارتها وتشغيلها.
=

الإنترنت على خوادم خارجية يديرها مزودو خدمات متخصصون، مما يوفر بديلًا عمليًا وفعالًا لوسائل التخزين مثل الأقراص الصلبة، وأجهزة التخزين المحمولة[١].

فهو يمتاز بقدرته على توفير مرونة فائقة، حيث يمكن للمستخدمين الوصول لبياناتهم بسهولة، شرط توفر اتصال بالشبكة العنكبوتية، وهذه الميزة تعزز الإنتاجية، وتلبي الاحتياجات التي تتطلب التنقل والعمل عن بعد. كما أنه يقدم حلًا فعالًا من حيث التكلفة، إذ يتم دفع تكاليف التخزين على أساس السعة المستخدمة دون الحاجة إلى استثمارات ضخمة في البنية التحتية[٢].

=

في سبعينيات القرن العشرين، ساهمت أجهزة الحاسوب الصغيرة مثل سلسلة PDP وVAX من شركة Digital Equipment في توسيع استخدام الحوسبة داخل الأعمال والأوساط الأكاديمية. هذه الأجهزة كانت أقل تكلفة وأسهل في الإدارة، مما أتاح للشركات الصغيرة والأكاديميات إمكانية الوصول إلى الحوسبة.

وفقًا للمخترع جون مكارثي، حل تقاسم الوقت مشكلة الحاجة إلى حواسب رئيسية كبيرة. وسمح نظام التشغيل المخصص لتقاسم الوقت للعديد من المستخدمين بالوصول المتزامن إلى حاسب آلي رئيسي كبير وقوي يتم مشاركته من خلال محطات طرفية بعيدة. وهذا الأسلوب أتاح الاستفادة القصوى من الموارد المتاحة وقدم حلاً فعالًا.

مع تطور التكنولوجيا، شهدنا تحولًا من الحواسب الرئيسية الكبيرة إلى الحوسبة السحابية الحديثة. هذا التطور يعكس القدرة على الابتكار المستمر والبحث عن حلول أفضل لتلبية احتياجات الشركات والأكاديميات المختلفة. الحوسبة السحابية اليوم تقدم مرونة وكفاءة عالية، مما يجعلها الخيار الأمثل للعديد من الشركات في مختلف القطاعات.

(1) R. Kanna, D. Lakshmi, P. Muneeshwari, G. M. Valantina & R. Suguna. (2024). Enhancing Enterprise Data Management with Secure and Scalable Cloud Storage Solutions. 2024 Second International Conference on Advances in Information Technology (ICAIT), Chikkamagaluru, Karnataka. India. PP 1 – 6. doi: 10.1109/ICAIT61638.2024.10690776.

(2) Yaser Mansouri, Adel Nadjaran Toosi, & Rajkumar Buyya. (2017). Data Storage Management in Cloud Environments: Taxonomy, Survey, and

=

على الرغم من الفوائد العديدة التي يقدمها التخزين السحابي، إلا أن هناك مخاوف متزايدة تتعلق بأمن البيانات والخصوصية. تخزين البيانات على خوادم بعيدة يتطلب ثقة عالية بمزودي الخدمة السحابية، مما يستوجب على المستخدمين فهم المخاطر، والعمل على تدابير مناسبة.

وبالتالي؛ يعد مفهوم التخزين السحابي، ركيزة أساسية في عصر المعلومات، حيث يقدم حلًا مثاليًا لإدارة البيانات بفعالية وكفاءة. ومع ذلك، فإن الاعتماد المتزايد عليه يتطلب وعيًا بالتحديات المرتبطة به لضمان تحقيق الاستفادة القصوى منه.

تعريف التخزين السحابي:

يشير مصطلح التخزين السحابي[١] إلى مجموعة واسعة من إمكانات التخزين التي يوفرها موفرو خدمات السحابة. وهذه الإمكانات تُتيح للمستخدمين، سواء كانوا أفرادًا أو شركات، تخزين البيانات على أجهزة تتم إدارتها، من قبل مزودي الخدمة. فالتخزين السحابي تقنية حديثة أحدثت تحولًا جذريًا في كيفية تخزين

=

Future Directions. ACM Computing Surveys (CSUR). Vol 50. Iss 6. PP 1 – 50. https://doi.org/10.1145/3136623.

(١) مصطلح "السحابة" يُستخدم عادةً للإشارة إلى "الإنترنت"، لذا يُطلق على "الحوسبة السحابية" أيضًا اسم "الحوسبة عبر الإنترنت". والحوسبة السحابية هي وسيلة لتجميع ومشاركة الموارد من الأجهزة والبرمجيات على نطاق واسع.

والشركات التي تقدم هذه الخدمات تُسمى مزودي الخدمات السحابية، وعادة ما يتم فرض رسوم على خدمات الحوسبة السحابية بناءً على الاستخدام، أي أن التكلفة تتناسب مع مقدار الخدمات أو الموارد التي يستخدمها العميل.

Matthew N. O. Sadiku, Chandra M. M. Kotteti & Janet O. Sadiku. (2024). Cloud Computing Law: An Introduction. International Journal of Trend in Research and Development, Vol 11. Iss 3. P 176. ISSN: 2394-9333

البيانات والوصول إليها، وهذه التقنية تعتمد على تخزين البيانات والمعلومات على خوادم بعيدة يديرها مزودو خدمات السحابة بدلًا من تخزينها محليًا على أجهزة تقليدية[١].

فالتخزين السحابي يسمح للوصول إلى البيانات من خلال الإنترنت باستخدام أي جهاز متصل، وضمان عدم فقدها بسهولة نتيجة تلف وحدات التخزين الخاصة بالمستخدمين، ما يمنح المستخدمين مرونة غير مسبوقة. يتميز التخزين السحابي بمرونته وفعاليته من حيث التكلفة، حيث يُمكن العملاء من الدفع فقط مقابل الموارد التي يستهلكونها. وبفضل التخزين السحابي، لم يعد المستخدم مقيدًا بجهاز واحد أو موقع معين للوصول إلى معلوماته. بل أصبح الآن تبادل البيانات بسهولة والعمل عليها بشكل مشترك من أماكن متعددة، مهما بلغ حجم تلك البيانات، فالتخزين، مما يعزز الإنتاجية، ويساهم في خلق بيئة عمل أكثر انفتاحًا وتكاملًا. وبالإضافة إلى ذلك، يوفر التخزين السحابي مستويات عالية من الأمان ونسخ احتياطي تلقائي للبيانات، ما يقلل من أخطار الفقدان أو التلف[٢]. تتمثل أبرز مميزاته فيما يلي[٣]:

(1) Ibid. PP 176 – 180.

(2) Zephrina C. & J Bhuvana. (2024). Revolutionizing Cloud Storage Security: Searchable Public-Key Encryption. International Journal of Innovative Research in Computer and Communication Engineering. Vol 12. Iss 3. PP 1883 – 1888. https://doi.org/10.15680/ijircce.2024.1203085.

(3) V.G, P.A. (2024). SecureLaw Portal: Empowering Citizens with Transparent Legal Records via Blockchain and Cloud eVault. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT. Vol 8. Iss 12. ISSN: 2582-3930.

١- **الوصول المرن والسهل:** يوفر التخزين السحابي إمكانية الوصول إلى البيانات، من أي مكان عبر الإنترنت، مما يجعله خيارًا مثاليًا للأفراد والشركات التي تعمل أثناء التنقل أو من مواقع متعددة.

٢- **قابلية التوسع:** يمكن للمستخدمين تخصيص مساحة التخزين وفقًا لاحتياجاتهم دون القلق من نفاد المساحة. سواء كنوا أفرادًا أو مؤسسات صغيرة كبرى، يمكنك زيادة أو تقليل السعة بسهولة.

٣- **الأمان المحسن:** تعتمد خدمات التخزين السحابي قواعد أمان عالية، مما يحمي البيانات من التهديدات، والضياع.

٤- **توفير النفقات**: يُعتبر التخزين السحابي حلًا اقتصاديًا، وذلك مقارنة بالاستثمار في البنى التحتية التقليدية. إذ يمكن الدفع على أساس الاستخدام، مما يُجنب المستخدمين تكاليف الصيانة والتشغيل.

٥- **التعاون الفعّال:** يوفر التخزين السحابي بيئة مثالية للتعاون بين الفرق، إذ يُتيح مشاركة الملفات والموارد في الوقت الفعلي، مما يُعزز الإنتاجية والكفاءة في العمل الجماعي.

٦- **تطبيقات متعددة:** تتجاوز استخدامات التخزين السحابي مجرد تخزين البيانات، إذ يستخدم في إدارة البيانات الضخمة، والتحقيقات الرقمية، مما يوسع آفاق استخدامه في مختلف المجالات.

ومع هذه الميزات، يُعد التخزين السحابي خيارًا استراتيجيًا للأفراد والشركات الذين يسعون لتحقيق كفاءة أكبر، أمان أفضل، وتوفير في التكاليف. إنه التقنية التي تمهد الطريق لمستقبل يعتمد على المرونة والابتكار.

أنواع التخزين السحابي:

تُصمم إمكانات التخزين السحابي لتلبية متطلبات مختلفة، سواء كانت تخزين البيانات بكميات كبيرة، وذلك من خلال بيئة مرنة لتخزين النسخ الاحتياطية، أو لدعم التطبيقات التي تتطلب أداءً عاليًا. وبالرغم من اختلاف الأهداف، إلا أن جميع هذه الإمكانات تمكن العملاء من استخدام الموارد وفقًا لاحتياجاتهم الفعلية.

ولتلبية تلك المتطلبات، فإن هناك أنواع متعددة من التخزين السحابي للبيانات، تختلف بناءً على الغرض من الاستخدام وطريقة تقديم الخدمة. وفيما يلي الأنواع الرئيسية للتخزين السحابي:

١- **التخزين السحابي العام**: التخزين السحابي العام هو أحد الأنواع الأكثر شيوعًا للتخزين السحابي، حيث يتم توفيره من قبل مزودي خدمات سحابية معروفين، حيث خدمات تخزين يقدمها مزودو الطرف الثالث عبر الإنترنت مثل Google Drive وDropbox وAmazon S3. وفي هذا النوع من التخزين، تُخزن البيانات على خوادم مشتركة تُدار بواسطة مزود الخدمة(١).

ويتميز التخزين السحابي العام بخصائص رئيسية تجعله خيارًا مناسبًا لمجموعة واسعة من الاستخدامات. فهو يوفر الوصول إلى البيانات من أي مكان باستخدام اتصال بالإنترنت، ويُعد سهل الاستخدام بفضل واجهته البسيطة التي تُناسب الأفراد والشركات الصغيرة. بالإضافة إلى ذلك، يتميز هذا النوع من

(1) Manju K. Mathai & Juby Mathew. (2024). Chapter Cloud storage (Implementing a third-party public auditing scheme). In Book Research Advances in Network Technologies. Taylor & Francis Group. 1st Edition. PP 18 and beyond. E-ISBN9781003433958.

التخزين بتكلفته المنخفضة، حيث يدفع المستخدمون فقط مقابل المساحة التي يستخدمونها[١].

وبالتالي؛ يُعد التخزين السحابي العام عمليًا للتخزين الشخصي كحفظ الصور، والمستندات، والفيديوهات، كما يُستخدم على نطاق واسع في المشاريع الصغيرة لتخزين البيانات ومشاركتها بين أعضاء الفريق. علاوة على ذلك، يُعتبر وسيلة فعالة للنسخ الاحتياطي للملفات المهمة.

وبالرغم من مزاياه، فإن التخزين السحابي العام يواجه بعض العيوب، مثل مشاركة البنى التحتية بين المستخدمين، مما قد يزيد من أخطار الأمان في حالة الهجمات السيبرانية. كما يعتمد بشكل كامل على الإنترنت للوصول إلى البيانات، وقد تكون خيارات التخصيص محدودة مقارنة بأنواع أخرى من التخزين[٢].

٢- **التخزين السحابي الخاص**: يُعتبر التخزين السحابي الخاص خيارًا مخصصًا حيث تُستخدم الموارد السحابية من قِبل مؤسسة واحدة فقط، وفيه يتم تخصيص الخوادم والموارد السحابية بشكل كامل لهذه المؤسسة، مما يتيح لها مستوى أعلى من الأمان

(1) Babu M.R., Nikhitha T., Naheeda S., Kethan S., Sainath P. & Jaswanth, V. (2023). A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage. In: Choudrie J., Mahalle P.N. Perumal T., Joshi A. (eds) IOT with Smart Systems. ICTIS 2023. Lecture Notes in Networks and Systems. Springer, Singapore. Vol 720. PP 217–228. https://doi.org/10.1007/978-981-99-3761-5_21.

(2) G. M., et. al. (2021). A Comprehensive Analysis on Efficient Multimedia Storage Mechanism In Public Cloud Environment With Secured Access. Turkish Journal of Computer and Mathematics Education (TURCOMAT). Vol 12. Iss 5. PP 1273 – 1280. doi: 10.1007/978-981-99-3761-5_21.

والتحكم مقارنة بالتخزين السحابي العام. وتُدار هذه الخوادم إما داخليًا، أو من خلال مزود خدمة خارجي، مع ضمان الخصوصية للبيانات[١].

وللتخزين السحابي الخاص عدة خصائص رئيسية. أولها، أنه يتيح التخصيص الكامل، مما يمنح المؤسسات سيطرة شاملة على إعدادات التخزين وإدارة البيانات. وثانيها، تتمثل في توفر أمانًا محسّنًا، وذلك؛ بفضل تلك الإجراءات الأمنية، يوفر مستوى عالٍ من التحكم، حيث يُمكن للمؤسسات من تلبية احتياجاتها الخاصة[٢].

ويستخدم التخزين السحابي الخاص بشكل رئيسي في القطاعات الهامة. فعلى سبيل المثال، تعتمد الحكومات عليه لتخزين البيانات ذات السرية العالية. وأيضًا في الكيانات الكبيرة لإدارة البيانات الداخلية، وفي المشاريع التي تحتاج إلى تحكم كامل بالبنية التحتية[٣].

(1) Noopur Malse, Aditya Lad, Atharv Mandpe & Nishant Lanjewar. (2024). Developing a Secure Private Cloud Storage System. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Vol 12. Iss XI. PP 1419 – 1425. https://doi.org/10.22214/ijraset.2024.65348.

(2) Maha A. Sayal. (2023). Private Storage Cloud for Facilitate the Functions of Organizations. International Journal of Information Technology & Computer Engineering. Vol 3. Iss 6. PP 43 – 51. https://doi.org/10.55529/ijitc.36.43.51.

(3) Meiditra I., Yuhandri & Sumijan. (2023). ANALISIS DAN PERANCANGAN PRIVATE CLOUD STORAGE MENGGUNAKAN METODE IDS (INTRUSION DETECTION SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM) STUDI KASUS DINAS KOMUNIKASI DAN INFORMATIKA KOTA PADANG PANJANG. Riau Journal of Computer Science (RJOCS). Vol 9. Iss 2. PP 124 – 133. https://doi.org/10.30606/rjocs.v9i2.1781.

وبالرغم من الميزات العديدة التي يتمتع بها التخزين السحابي الخاص، مثل مستوى الأمان العالي ومرونة التخصيص والامتثال للتشريعات المتعلقة بحماية البيانات، إلا أن هناك بعض التحديات. منها التكلفة العالية، حيث يتطلب استثمارات كبيرة في البنية التحتية وإدارتها. بالإضافة إلى ذلك، تُعد إدارته معقدة نسبيًا، حيث تحتاج المؤسسات إلى فريق متخصص لصيانة وإدارة الخوادم(١).

٣- **التخزين السحابي الهجين**: يُعتبر التخزين السحابي الهجين حلًا مثاليًا يجمع بين مزايا التخزين السحابي العام والخاص. فهو يتيح للمؤسسات تخزين البيانات الحساسة في بيئة سحابية خاصة ذات مستوى عالٍ من الأمان، مع الاستفادة من السحابة العامة لتخزين البيانات الأقل حساسية أو التي تتطلب موارد تخزين مرنة(٢).

وأحد أبرز الخصائص المميزة للتخزين السحابي الهجين تتمثل في قدرته على تحقيق تكامل سلس بين التخزين العام والخاص، والذي يتيح نسخ البيانات، وتوزيعها حسب الحاجة. كما يسمح هذا النموذج للمؤسسات بالتوسع باستخدام موارد السحابة العامة عند الحاجة إلى سعة تخزين إضافية، دون التأثير البيانات المحفوظة في السحابة(٣).

---

(1) G. M., et. al. (2021). A Comprehensive Analysis on Efficient Multimedia Storage Mechanism In Public Cloud Environment With Secured Access. Op. cit. PP 1273 – 1280

(2) Debarpita Dutta. (2024). Secure Storage on Cloud using Hybrid Cryptography. International Journal of Advanced Research in Science, Communication and Technology. Vol 4. Iss 1. PP 62 -75. DOI: 10.48175/IJARSCT-18707.

(3) S. HR & T. S. (2021). A Hybrid Cloud Approach for Efficient Data Storage and Security. 2021 6th International Conference on Communication and Electronics Systems (ICCES). Coimbatre, India. PP 1072 – 1076. doi: 10.1109/ICCES51350.2021.9488938.

ويُستخدم التخزين السحابي الهجين بشكل شائع في المشروعات التي تحتاج إلى تخزين بيانات ضخمة، مع تخصيص السحابة الخاصة للبيانات الحساسة، مثل بيانات العملاء، أو السجلات المالية. كما يُعد خيارًا مناسبًا للقطاعات الحساسة، التي تتطلب معادلة دقيقة بين الأمان والمرونة. بالإضافة إلى ذلك، يمكن استخدام هذا النوع من التخزين لإدارة الأعباء المؤقتة، مثل تخزين البيانات المؤقتة أثناء فترات الذروة[١].

ويوفر التخزين السحابي الهجين العديد من المزايا، منها الأمان المعزز، وبفضل الحماية الفائقة للبيانات في السحابة الخاصة، وخفض التكاليف. ويتميز بمرونة عالية تمكن الكيانات من التوسع عند الطلب. ومع ذلك، فإنه يواجه بعض التحديات، مثل التعقيد في الإدارة، حيث يتطلب التنسيق بين السحابتين العامة والخاصة خبرة تقنية وإدارة فعّالة. بالإضافة إلى ذلك، قد تكون التكلفة الأولية لإنشاء البنية التحتية الخاصة مرتفعة، كما يتطلب أمان البيانات أثناء نقلها بين السحابتين عناية خاصة وفائقة[٢].

٤- **التخزين السحابي الموزع**: التخزين السحابي الموزع هو نوع من التخزين السحابي يتم فيه توزيع البيانات عبر عدة مواقع جغرافية أو خوادم منفصلة. والهدف من هذا النموذج هو تحسين الأمان والموثوقية من خلال ضمان أن البيانات ليست مخزنة في

(1) Nagappan Mageshkumar, J. Swapna, A. Pandiaraj, R. Rajakumar, Moez Krichen & Vinayakumar Ravi. (2023). Hybrid cloud storage system with enhanced multilayer cryptosystem for secure deduplication in cloud. International Journal of Intelligent Networks. Vol 4. PP 301-309. ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2023.11.001.

(2) S. HR & T. S. (2021). A Hybrid Cloud Approach for Efficient Data Storage and Security. Op. cit. PP 1072 – 1076.

موقع واحد فقط. وهذا التوزيع يقلل من أخطار فقدان البيانات الناتج عن الأعطال الفنية أو الهجمات السيبرانية، ويُسهم في تحسين الأداء العام للنظام[١].

وأحد أبرز الخصائص الرئيسية للتخزين السحابي الموزع هو التوزيع الجغرافي للبيانات، إذ يتم توزيع البيانات على أماكن مختلفة. وهذا يعزز من الأمان ويضمن استمرارية الخدمة حتى في حالة تعطل أحد المواقع. بالإضافة إلى ذلك، يُسهم التخزين السحابي الموزع في تحسين الأداء من خلال تقليل زمن الوصول، حيث يتم استرداد البيانات من أقرب خادم للمستخدم[٢].

ويُستخدم هذا النوع في العديد من المجالات، مثل التطبيقات التي تتطلب توفير البيانات على مستوى عالمي، مثل منصات البث. ولذلك يُعد خيارًا مثاليًا لأنظمة معالجة البيانات الضخمة، إذ يتيح تخزين ومعالجة البيانات عبر مواقع متعددة. بالإضافة إلى ذلك، يُستخدم في أنظمة النسخ الاحتياطي، وهذا يمكن من استرداد البيانات بسرعة وفعالية في حالة حدوث أي خلل[٣].

(1) Q. Dong J. Tang S. Dang G. Chen & J. A. Chambers. (2023). Blockchain-Assisted Reputation Mechanism for Distributed Cloud Storage," in IEEE Systems Journal. Vol 17. Iss 4. PP 6334 – 6345. doi: 10.1109/JSYST.2023.3277194.

(2) Meesala Sravani & Meesala Krishna Murthy. (2023). REDUCTION OF DATA LEAKAGE IN DISTRIBUTED CLOUD STORAGE SYSTEMS USING DISTRIBUTED CLOUD GUARD (DCG). INDIAN JOURNAL OF COMPUTER SCIENCE AND ENGINEERING. Vol 14. Iss 3. PP 444 - 450. ISSN: 0976-5166. https://doi.org/10.21817/indjcse/2023/v14i3/231403014.

(3) Chun-Li Ma., Dong-Dong Li., Yalin Li., Yinghao Wu., Song-Yan Ding., Jun Wang., Pei-Yuan Li., Song Zhang, Junjie Chen, Xiaoxing Zhang, Jia-Yong, Wang, Jin Li., Qiang Li., Zhi-Tong Chen, Lei Zhou, Mei-Sheng =

ومن بين مزايا التخزين السحابي الموزع، تعزيز الأمان من خلال توزيع البيانات، مما يُقلل الوصول غير المصرح به، أو فقدها. ويُوفر مرونة من أجل التوسع. كما يُسهم توزيع البيانات جغرافيًا، أيضًا في تقليل زمن الوصول، حيث يتم استرداد البيانات من أقرب خادم. علاوة على ذلك، يضمن هذا النموذج استمرارية الخدمة حتى في حالة تعطل أحد المواقع(١).

على الرغم من مزاياه، يواجه التخزين السحابي الموزع بعض التحديات. ومن أبرزها التعقيد في إدارة البيانات بين المواقع المختلفة، حيث يتطلب ذلك تقنيات وخبرات متقدمة. بالإضافة إلى ذلك، تُعتبر التكلفة التشغيلية عالية نتيجة الحاجة إلى تشغيل وإدارة خوادم متعددة في أماكن مختلفة. كما أن نقل البيانات بين المواقع الجغرافية المختلفة قد يُعرضها للمخاطر الأمنية إذا لم تُستخدم تقنيات حماية قوية، أو القانونية والتي تتمثل في اختلاف القوانين الخاصة بالبيانات بين الدول(٢).

٥- **التخزين السحابي القائم على الكائنات (Object Storage)**: يُعتبر التخزين السحابي القائم على الكائنات أو "المرتكز على التطبيقات"، وهو من أكثر أنواع

=

Zhao, Yong Zhao. (2023). Quantum-secure fault-tolerant distributed cloud storage system. AIP Advances. Vol 13. Iss 11. 115309. https://doi.org/10.1063/5.0172384.

(1) Yogesh Gupta. (2021). Novel distributed load balancing algorithms in cloud storage. Expert Systems with Applications. Vol 186. 115713. ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2021.115713.

(2) A. M. Shuvo, M. S. Amin & P. Haque. (2020). Storage Efficient Data Security Model for Distributed Cloud Storage. 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC). Kuching, Malaysia. PP 1 - 6. doi: 10.1109/R10-HTC49770.2020.9356962.

التخزين السحابي شيوعًا لتخزين البيانات الضخمة غير الهيكلية، مثل الفيديوهات، المستندات، وملفات الوسائط الأخرى. وفيه يتم تخزين البيانات على شكل كائنات مستقلة، حيث يحتوي كل كائن على البيانات نفسها، والبيانات الوصفية (Metadata)، ومعرّف فريد يُسهّل الوصول إليها وإدارتها.

وأحد أبرز خصائص التخزين القائم على الكائنات هو قدرته على التعامل مع البيانات غير الهيكلية بكفاءة عالية. حيث يتم تنظيم البيانات ككائنات مستقلة مع بيانات وصفية غنية تُسهل البحث عنها وتصنيفها. بالإضافة إلى ذلك، يُوفر التخزين القائم على الكائنات مرونة هائلة في التوسع(١).

ويُستخدم التخزين القائم على الكائنات في تخزين الوسائط الرقمية مثل الصور، والمستندات على المنصات الرقمية، أو البث الحي. ويُعتبر خيارًا عمليًا لأرشفة البيانات طويلة الأمد مثل السجلات الطبية وأرشيفات البريد الإلكتروني. بالإضافة إلى ذلك، يتم اعتماده لتخزين النسخ الاحتياطية للبيانات الكبيرة واستخدامه في تحليل البيانات الضخمة في تطبيقات البحث العلمي(٢).

(1) Dieckmann M. A., Beyvers S., Hochmuth J., Rehm A., Förster F., & Goesmann A. (2023). The Aruna Object Storage: A Distributed Multi Cloud Object Storage System for Scientific Data Management. Proceedings of the Conference on Research Data Infrastructure. Vol 1. https://doi.org/10.52825/cordi.v1i.404.

(2) Mondal A.S., Mukhopadhyay A. & Chattopadhyay S. (2022). Machine learning-driven automatic storage space recommendation for object-based cloud storage system. Complex Intell. Syst. Vol 8. PP 489 – 505. https://doi.org/10.1007/s40747-021-00517-4.

وأحد أشهر الأمثلة على هذا النوع من التخزين هو Amazon S3، الذي يُوفر تخزينًا مرنًا وقابلًا للتوسع مع ميزات أمان قوية. ومن الأمثلة الأخرى Google Cloud Storage، الذي يُقدم خدمات مشابهة مع إمكانية التكامل مع أدوات تحليل البيانات المختلفة(١).

ومن أهم مزايا التخزين القائم على الكائنات هي قابليته للتوسع الهائل، حيث يُمكن تخزين كميات ضخمة من البيانات دون قيود على الحجم أو عدد الكائنات. فالبيانات المدمجة تمكن من إدارة البيانات بفعالية. إضافة إلى ذلك، يُعتبر هذا النوع أقل تكلفة عند تخزين كميات كبيرة من البيانات ويوفر سهولة في التكامل مع التطبيقات الحديثة(٢).

ومع ذلك، يواجه التخزين القائم على الكائنات بعض التحديات. قد يكون أداؤه محدودًا مع البيانات الصغيرة، كما أن استرجاع البيانات يمكن أن يكون أبطأ مقارنة بأنواع التخزين الأخرى. بالإضافة إلى ذلك، هناك بعض التطبيقات التقليدية لا تتوافق مع هذا النموذج(٣).

(1) Dieckmann M. A., Beyvers S., Hochmuth J., Rehm A., Förster F., & Goesmann A. (2023). The Aruna Object Storage: A Distributed Multi Cloud Object Storage System for Scientific Data Management. Op. cit.

(2) N. Manubens, S. D. Smart, T. Quintino & A. Jackson. (2022). Performance Comparison of DAOS and Lustre for Object Data Storage Approaches. 2022 IEEE/ACM International Parallel Data Systems Workshop (PDSW). Dallas. TX. USA. PP 7 - 12. doi: 10.1109/PDSW56643.2022.00007.

(3) Mondal A.S., Mukhopadhyay A. & Chattopadhyay S. (2022). Machine learning-driven automatic storage space recommendation for object-based cloud storage system. Op. cit. PP 489 – 505

٦- **تخزين السحابة العالية الأداء**: يعتبر هذا النوع من التخزين من العوامل التي تحسين من فعالية العديد من التطبيقات، مثل الذكاء الاصطناعي، المحاكاة الهندسية. مع تقدم التقنيات في السنوات الأخيرة، أصبحت الحوسبة عالية الأداء في السحابة أكثر سهولة وتوفرًا من حيث التكلفة، وهذا يمكن من الاستفادة من هذه القدرات بشكل كبير[١].

وأحد العقبات التي تواجه هذا النوع، تتعلق بإنتاجية نظام الملفات المشترك. كانت هذه الأنظمة في السابق تمثل عقبة أمام الأداء الفعال في العمليات المعقدة مثل المحاكاة وتطبيقات الذكاء الاصطناعي. ولكن مع التكوينات والمواصفات الصحيحة، يمكن دعم هذه الأحمال بكفاءة عالية[٢].

ويتم دعم هذه التطبيقات من خلال تخزين الكتل المدعوم بواسطة وسائط SSD وتقنيات مراكز البيانات الحديثة مثل NVMe، مما يوفر سرعة عالية واستقرارًا في الشبكات. ويمكن لهذا الأداء العالي أن يضمن تحقيق أعلى مستويات الإنتاجية وأقل زمن وصول[٣].

(1) Marquez J., & Mondragon O. H. (2024). Modelling the Impact of Cloud Storage Heterogeneity on HPC Application Performance. Computation. Vol 12. Iss 7. https://doi.org/10.3390/computation12070150.

(2) Loris Belcastro, Fabrizio Marozzo & Paolo Trunfio. (2024). Infrastructures for High-Performance Computing: Cloud Computing. Reference Module in Life Sciences. Elsevier. ISBN: 9780128096338. https://doi.org/10.1016/B978-0-323-95502-7.00005-1.

(3) Petrosyan D. & Astsatryan H. (2022). Serverless High-Performance Computing over Cloud. Cybernetics and Information Technologies. Sciendo. Vol 22. Iss 3. PP 82 - 92. https://doi.org/10.2478/cait-2022-0029.

إضافة إلى ذلك، يوفر تخزين الكتل من Oracle مستوى خدمة فريد من نوعه يمكنه أن يدعم احتياجات تخزين البيانات الكبيرة والمتطلبات الدقيقة لتطبيقات HPC، وعلى الرغم من أن هذا يتطلب التكوين اليدوي لمجموعات خادم الملفات على محركات الأقراص الصلبة المرتبطة مباشرة بها(١).

كل نوع من هذه الأنواع له مزاياه وعيوبه، ويعتمد الاختيار على احتياجات المستخدم أو المؤسسة. فإذا كانت المستخدم بحاجة إلى مرونة في الموارد وقادرة على تحمل تكاليف التشغيل المتغيرة، فقد تكون الحوسبة السحابية خيارًا أفضل. أما إذا كانت الحاجة تقتصر على أداء ثابت وعالي مع ضرورة التحكم الكامل في البيئة، فقد يكون التخزين المحلي في بيئة معتمدة على وحدات تخزين من نوع SSD وNVMe هو الخيار الأنسب. فالاختيار بين هذه الخيارات يعتمد على أولويات المستخدم أو المؤسسة.

الأبعاد التقنية والقانونية للتخزين السحابي:

تتشابك الأبعاد التقنية والقانونية للتخزين السحابي، مما يوفر فرصًا وتحديات للمستخدمين ومقدمي الخدمات. ومع تزايد اعتماد المؤسسات للحلول السحابية لتلبية احتياجات الخاصة، يصبح فهم التدابير الأمنية والأطر القانونية أمرًا ضروريًا. سوف تستكشف هذه النظرة العامة الجوانب التقنية للتخزين السحابي والآثار القانونية والتقاطع بين البعدين.

فتقنيات التخزين السحابي تتيح للمستخدمين تخزين بياناتهم وإدارتها على خوادم خارجية، مما يوفر مزايا متعددة. ومن أبرز هذه المزايا تشمل الوصول المرن،

(1) Petrosyan D. & Astsatryan H. (2022). Serverless High-Performance Computing over Cloud. Cybernetics and Information Technologies. Op. cit. PP 82 - 92

الذي يُمكّن المستخدمين من التعامل مع بياناتهم في الوقت المطلوب، ومن أي مكان يتم التواجد فيه. ويضيف مستوى من الأمان المحسن، وذلك باستخدام التشفير الكامل، لضمان حماية وأمن البيانات. بالإضافة إلى ذلك، تبرز المرونة والقابلية للتوسع كميزات جوهرية، حيث يمكن تخصيص الموارد حسب احتياجات المستخدمين دون قيود على السعة أو الأداء(١).

من الناحية القانونية، يتطلب الاعتماد المتزايد على التخزين السحابي تنظيم العلاقة بين المستخدمين ومزودي الخدمة. وهنا؛ تُعد قوانين حماية البيانات، الركائز لضمان حقوق المستخدمين وخصوصيتهم، بينما تسعى الالتزامات التعاقدية إلى تحديد مسؤوليات مقدمي الخدمة عن أمان البيانات وسلامتها. علاوة على ذلك، تبرز تحديات الامتثال الدولي في ظل اختلاف القوانين بين الدول، مما يفرض ضرورة التنسيق بين الأطر القانونية المختلفة(٢).

وبالتالي؛ يمثل الجانب التقني والقانوني في التخزين السحابي للبيانات مجالًا يوفر فرصًا كبيرة، مثل تعزيز الأمان وابتكار حلول جديدة لحماية الخصوصية. ومع ذلك، هناك عقبات كبيرة يفرضها، بما في ذلك أخطار الاختراقات الأمنية والتضارب

(1) Patnaik S., Garikapati K., Dash L., Bhattacharya R., & Mohapatra A. (2024). Safeguarding Patient Privacy: Exploring Data Protection in E-Health Laws: A Cross-Country Analysis. EAI Endorsed Transactions on Pervasive Health and Technology. Vol 10. https://doi.org/10.4108/eetpht.10.5583.

(2) Adhab A. H., & Hussien N. A. (2023). Study of Efficient Cloud Storage Architectures for the Security Environment. Journal of Kufa for Mathematics and Computer. Vol 10. Iss 1. PP 63 – 71. https://doi.org/10.31642/JoKMC/2018/100108.

التشريعي بين الدول المختلفة. بالإضافة إلى ذلك، هناك حاجة ملحّة لتوعية المستخدمين والمؤسسات بحقوقهم ومسؤولياتهم القانونية لتحقيق أقصى استفادة من التقنيات، مع تقيل التهديدات المتعلقة بها.

٢,١. الأبعاد التقنية للتخزين السحابي:

التخزين السحابي يقوم على تقنيات متعددة لضمان تقديم خدمات تخزين عالية الكفاءة والأمان، ومن خلالها يمكن للمستخدمين الاستفادة من موارد التخزين بشكل مرن وفعال، مما يعزز من إنتاجيتهم ويحمي بياناتهم الحساسة. وتشمل الأبعاد التقنية مجموعتنا نوعيتنا من الأبعاد. فالمجموعة الأولى تشمل توفير خدمات التخزين بكفاءة وأمان، والمجموعة الثانية خاصة بالتدابير الفنية المطبقة على خدمات التخزين السحاب ومتطلبات الأمان بها. وفيما يلي بيان لكل مجموعة(١).

٢,١,١ الأبعاد التقنية للتخزين السحابي الخاصة بالكفاءة وأمان:

التخزين السحابي يقوم على تقنيات متعددة لضمان تقديم خدمات تخزين عالية الكفاءة والأمان. وهذه الأبعاد تشمل الأمان السيبراني لضمان حماية البيانات، وبفضل هذه الأبعاد المتكاملة، يوفر التخزين السحابي حلولاً مثالية للأفراد والشركات في العصر الرقمي. وهذه الأبعاد تشمل العناصر التالية:

(1) Harsh Deo Ravi, Tejas Mittal, Gaurav, Sachin Kumar, Anoop Singh & Aadil Feroz. (2024). Secure and Efficient Cloud Storage System with Deduplication and Compression Using Blockchain Technology. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Vol 45. Iss 98. PP 447 – 455. https://doi.org/10.22214/ijraset.2024.65086.

١- **البنية التحتية**: التخزين السحابي يعتمد على شبكات واسعة من الخوادم المنتشرة في مراكز بيانات متطورة حول العالم. وهذه المراكز يجب أن تكون مجهزة لتوفير الأداء العالي والقدرة على التعامل مع كميات هائلة من البيانات. كما يجب أن يتم تصميم هذه المراكز لضمان استقرار الخدمة وتقديم أفضل أداء ممكن للمستخدمين(١).

والوصول إلى خدمات التخزين السحابي يتم عبر الإنترنت، مما يجعل البنى التحتية للشبكة العنكبوتية عنصر هامًا لها. إذ تقوم خدماتها على الشبكات عالية السرعة والموثوقة لضمان الوصول الآمن للبيانات. ويجب أن تتمكن الشبكات من نقل البيانات بسرعة وأمان(٢).

٢- **التوافر والمرونة:** يجب أن توفر خدمات التخزين السحابي القدرة على التوسع التلقائي وفقًا لاحتياجات المستخدم، سواء من ناحية قدرات التخزين أو كفاءة الأداء. وهذا يعني أن المستخدمين يمكنهم زيادة سعة التخزين أو تحسين الأداء بسهولة عند الحاجة، دون الحاجة إلى شراء معدات جديدة أو إجراء تعديلات معقدة(٣).

(1) Gupta Y. (2021). Novel distributed load balancing algorithms in cloud storage. Expert Syst. Appl. Vol 186. 115713. ISSN 0957-4174. https://doi.org/10.1016/J.ESWA.2021.115713.

(2) Rangaswamy K., Gurusamy M., & Vijayakumar P. (2020). An Efficient Cloud Data Center Allocation to the Source of Requests. J. Organ. End User Comput. Vol 32. Iss 3. PP 23 - 36. https://doi.org/10.4018/joeuc.2020070103.

(3) V.G, P.A. (2024). SecureLaw Portal: Empowering Citizens with Transparent Legal Records via Blockchain and Cloud eVault. Op. cit.

كما يجب أن تضمن تقنياته الوصول إلى البيانات. وذلك عن طريق البنى التحتية الموزعة وتقنيات النسخ الاحتياطي المتقدمة، بحيث يمكن للمستخدمين الاطمئنان إلى أن بياناتهم ستكون متاحة دائمًا، حتى في حالة حدوث مشاكل في مراكز البيانات(١).

٣- **التقنيات المستخدمة في التخزين**: وتشمل:

- **التخزين القائم على الكتل (Block Storage):** وهذا يُستخدم لتقسيم البيانات إلى كتل منفصلة تُخزن على الخوادم. وهذا النوع من التخزين مناسب للتطبيقات التي تتطلب أداءً عاليًا وزمن وصول منخفض، مثل تطبيقات التخزين عالية الأداء. مما يوفر أداءً عاليًا، وسرعة في الحصول إلى البيانات، مما يجعله عمليًا للتطبيقات الحساسة للزمن(٢).

- **التخزين القائم على الملفات (File Storage):** وفيه يتم تخزين البيانات كملفات في هياكل تنظيمية مثل المجلدات. هذا النوع من التخزين مناسب للتطبيقات التي تحتاج إلى مشاركة المعلومات، كمشاركة مستندات العمل والمشاريع التعاونية. مما يتيح الحصول على المعلومات بسهولة(٣).

(1) Meesala Sravani & Meesala Krishna Murthy. (2023). REDUCTION OF DATA LEAKAGE IN DISTRIBUTED CLOUD STORAGE SYSTEMS USING DISTRIBUTED CLOUD GUARD (DCG). Op. cit. PP 444 - 450.

(2) Tak, B., Tang, C., Chang, R., & Seo, E. (2021). Block-Level Storage Caching for Hypervisor-Based Cloud Nodes. IEEE Access. Vol 9. PP 88724 - 88736. https://doi.org/10.1109/ACCESS.2021.3090308.

(3) Latha, D.S. (2022). SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY. International Research Journal of Modernization in Engineering Technology and Science. Vol 4. Iss 12. PP 1282 – 1290. https://www.doi.org/10.56726/IRJMETS32383.

توفر تقنيات التخزين المتنوعة حلولًا مختلفة كالأداء، وسهولة الإدارة. واختيار التقنية يعتمد على احتياجات التطبيقات والمستخدمين لضمان أفضل أداء وكفاءة في إدارة البيانات[١].

٤- **الأمان والخصوصية**: فاستخدام التشفير، لحماية البيانات أثناء النقل وعند تخزينها. يضمن هذا أن البيانات محمية، وأنها تظل سرية، وآمنة في جميع الأوقات[٢].

كما توفر خدمات التخزين السحابي نسخًا احتياطية بشكل دورية للبيانات، وذلك لضمان استعادتها. وهذا يساعد في الحفاظ على البيانات من الفقدان أو العبث غير المتوقع بها. كما يجب التحكم فيمن يمكنه الوصول إلى البيانات باستخدام تقنيات التوثيق وإدارة الصلاحيات. وهذا يضمن أن من يملك التصريح فقط، يمكنهم الوصول إلى البيانات، مما يعزز من مستوى الأمان والخصوصية[٣].

فمن خلال التركيز على الأمان والخصوصية، تضمن خدمات التخزين السحابي حماية البيانات وحفاظها على سرية وأمان تامين. فالتشفير، والنسخ الاحتياطي، وإدارة الوصول هي بعض من الأبعاد الرئيسية التي تساعد في تحقيق هذه الأهداف.

---

(1) Zichichi M., Ferretti S. & D'angelo G. (2020). On the Efficiency of Decentralized File Storage for Personal Information Management Systems. 2020 IEEE Symposium on Computers and Communications (ISCC). PP 1 - 6. https://api.semanticscholar.org/CorpusID:220381264.

(2) Ляпунов Б.А. (2019). Приватность личности: понятие, сущность и правовая природа. Актуальные проблемы российского права. Vol 2. PP 33 - 42. https://doi.org/10.17803/1994-1471.2019.99.2.033-042.

(3) L. Ma, W. Su, B. Wu, B. Yang and X. Jiang. (2022). Joint Emergency Data and Service Evacuation in Cloud Data Centers Against Early Warning Disasters. IEEE Transactions on Network and Service Management. Vol 19. Iss 2. PP 1306 - 1320. https://doi.org/10.1109/tnsm.2022.3147247.

٥- **التكامل مع الأنظمة الأخرى**: تسهل (APIs)[١] التكامل بين التخزين السحابي والتطبيقات أو الأنظمة الأخرى. تتيح هذه الواجهات للتطبيقات التواصل مع خدمات التخزين السحابي، مما يمكنها من تبادل البيانات والعمل بشكل متكامل[١].

---

(١) هي عبارة عن واجهة برمجة التطبيقات، ونعرف اختصارًا بـ API، وهي بمثابة وسيط أو رابط يمكّن برنامجين حاسوبيين مختلفين من التواصل والتفاعل مع بعضهما البعض. ويمكن تخيلها كموظف استقبال في فندق، يقوم بنقل طلباتك إلى الطاهي وإحضار الطلب إليك. في عالم البرمجة، تلعب APIs دورًا مشابهًا، حيث تنقل الطلبات بين تطبيقات مختلفة وتنقل النتائج مرة أخرى. وتعمل APIs عن طريق:

- **الطلب**: يرسل برنامج (تطبيق) طلبًا إلى API، يوضح فيه ما يريد الحصول عليه أو ما يريد أن يقوم به البرنامج الآخر.
- **المعالجة**: تستقبل API هذا الطلب وتقوم بمعالجته، ثم تتصل بالبرنامج الآخر لتنفيذ الطلب.
- **الرد**: يعود API بالنتيجة إلى البرنامج الأول الذي طلب الخدمة.

لماذا تعتبر APIs مهمة:

- تتيح APIs للمبرمجين بناء تطبيقات جديدة بشكل أسرع وأسهل، وذلك عن طريق الاستفادة من وظائف وبيانات تطبيقات أخرى موجودة مسبقًا.
- تعمل APIs على دمج وتوحيد العديد من التطبيقات المختلفة، مما يجعل العمل بينها أكثر سلاسة وكفاءة.
- تساهم APIs في تبسيط العمليات، مما يوفر الوقت والجهد.
- يمكن للشركات إنشاء مصادر دخل جديدة من خلال السماح لمطوري برامج آخرين باستخدام APIs الخاصة بها لبناء تطبيقات جديدة.

أمثلة على استخدام APIs في حياتنا اليومية:

وسائل التواصل الاجتماعي: عندما تقوم بمشاركة صورة من هاتفك على فيسبوك، فإن تطبيقك يستخدم API للتواصل مع منصة فيسبوك ونشر الصورة هناك.

تطبيقات الخرائط: تستخدم تطبيقات الخرائط APIs للحصول على بيانات عن المواقع والطرق من مصادر مختلفة.

التجارة الإلكترونية: تستخدم المتاجر الإلكترونية APIs للتكامل مع بوابات الدفع وشركات الشحن وإدارة المخزون.

تطبيقات الطقس: تحصل تطبيقات الطقس على بيانات الطقس من مصادر مختلفة عبر APIs.

=

ويمكن ربط التخزين السحابي مع أدوات إدارة البيانات لتحليل البيانات الكبيرة أو إجراء العمليات. وهذا التكامل يسمح بإدارة البيانات بشكل أكثر فعالية واستخدامها في تطبيقات الذكاء الاصطناعي(٢).

فالتكامل مع الأنظمة الأخرى قد يعزز من قدرات التخزين السحابي ويسهم في تحسين أداء التطبيقات والأنظمة المختلفة. وباستخدام APIs وأنظمة إدارة البيانات، يمكن تحقيق مستويات أعلى من الكفاءة والتعاون بين مختلف الأنظمة والتطبيقات.

٦- **الكفاءة والأداء**: تقنيات تحسين الأداء في التخزين السحابي تقوم على استخدام الأقراص الصلبة من النوع SSD، والتي توفر سرعة عالية في قراءة وكتابة

=

أنواع APIs:

- **APIs العامة**: متاحة لأي شخص يرغب في استخدامها.
- **APIs الخاصة**: تستخدم داخل شركة أو منظمة معينة.
- **APIs الشريكة**: يتم مشاركتها مع شركاء محددين.
- **APIs المستندة إلى REST**: تعتبر من أكثر أنواع APIs شيوعًا وتستخدم بروتوكول HTTP للتواصل.

Maxime Lamothe, Yann-Gaël Guéhéneuc, and Weiyi Shang. (2021). A Systematic Review of API Evolution Literature. ACM Comput. Surv. Vol 54. Iss 8. PP 1 - 36. https://doi.org/10.1145/3470133.

(1) Maxime Lamothe, Yann-Gaël Guéhéneuc, and Weiyi Shang. (2021). A Systematic Review of API Evolution Literature. Op. cit. PP 1 – 36.

(2) Latifian A. (2022). How does cloud computing help businesses to manage big data issues. Kybernetes. Vol 51. Iss 6. PP 1917 - 1948. https://doi.org/10.1108/k-05-2021-0432.

البيانات مقارنة بالأقراص التقليدية. بالإضافة إلى ذلك، تُستخدم شبكات NVMe لتقليل زمن الوصول، مما يعزز من سرعة الحصول عليها عند الحاجة[١].

ويتم تخزين البيانات بناءً على مستوى الاستخدام. بحيث تُخزن البيانات الأكثر أهمية والتي تحتاج إلى وصول سريع في الطبقات ذات الأداء العالي، في حين تُخزن البيانات الأقل أهمية في طبقات أقل تكلفة، ولكنها تتمتع بسعة تخزين أكبر[٢]. وهذا النهج يضمن كفاءة استخدام الموارد وتحسين الأداء حسب حاجة كل نوع من البيانات.

ومن خلال استخدام تقنيات تحسين الأداء والتخزين متعدد الطبقات، يوفر التخزين السحابي كفاءة عالية في إدارة البيانات وأداءً متفوقًا يلبي المتطلبات المختلفة للمتعاملين من خلالها.

٧- **تسعير الخدمات**: حيث يعتمد التسعير عادةً على الاستخدام الفعلي عن طريق:

- **كمية البيانات المخزنة**: يتم احتساب التكاليف بناءً على حجم البيانات المخزنة على السحابة. وزيادة كمية البيانات المخزنة، يقابله زيادة التكلفة[٣].

(1) Lee W., Kang M. & Kim S. (2024). Highly VM-Scalable SSD in Cloud Storage Systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol 43. Iss 1. PP 113 - 126. https://doi.org/10.1109/TCAD.2023.3305573.

(2) Abuhamra E., Ali E., & Ali E. (2024). Improving Cloud Database Performance Using Storage Technologies. IOSR Journal of Computer Engineering. Vol 26. Iss 5. PP 61 – 65. https://doi.org/10.9790/0661-2605036165.

(3) Yuan D., Cui L., Li W., Liu X. & Yang Y. (2018). An Algorithm for Finding the Minimum Cost of Storing and Regenerating Datasets in =

- **عدد الطلبات (Operations):** تكلفة استخدام خدمات التخزين السحابي يتم احتساب عدد الطلبات للوصول إلى البيانات أو تعديلها. وهذه الطلبات تشمل عمليات القراءة والكتابة والنقل(١).
- **سرعة نقل البيانات**: تشمل التكاليف أيضًا سرعة نقل البيانات. وكمية البيانات التي يتم نقلها، بالإضافة إلى سرعة الشبكة المطلوبة(٢).

ومن خلال التسعير الفعلي للخدمات، يتمكن المستخدمون من دفع تكاليف تتناسب مع احتياجاتهم الفعلية فقط، مما يوفر لهم مرونة كبيرة في إدارة تكاليف التخزين السحابي وتحقيق الاستفادة القصوى من الموارد المتاحة.

وهذه الأبعاد التقنية تعمل معًا لتوفير حلول تخزين موثوقة ومرنة للمستخدمين والشركات، مما يجعل التخزين السحابي خيارًا شائعًا لتلبية احتياجات البيانات المعاصرة.

٢,١,٢ الأبعاد الفنية المطبقة على خدمات التخزين السحاب ومتطلبات الأمان:

تعتمد خدمات التخزين السحابي على مجموعة من الأبعاد الفنية التي تضمن توفير الأداء العالي، المرونة، والأمان للمستخدمين. تشمل هذه الأبعاد استخدام تقنيات

=

Multiple Clouds. IEEE Transactions on Cloud Computing. Vol 6. Iss 2. PP 519 - 531. https://doi.org/10.1109/TCC.2015.2491920.

(1) Plewnia C. & Lichter H. (2023). Cross-provider Cloud Cost Calculation. 13th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2023). CEUR Workshop Proceedings; 3397. https://ceur-ws.org/Vol-3397/sci3.pdf.

(2) Zuo L. & Yun D. (2024). Optimal Balancing of Data Transfer Time and Cost in High-Performance Networks. 2024 International Conference on Computing, Networking and Communications (ICNC). PP 60 - 64. https://doi.org/10.1109/ICNC59896.2024.10556371.

متقدمة، لإدارة الوصول للبيانات، لضمان وصول المصرح لهم فقط إلى البيانات. وتساهم هذه الأبعاد الفنية ومتطلبات الأمان في تقديم خدمات تخزين سحابية عالية الكفاءة والموثوقية للمستخدمين في مختلف المجالات.

١- **السرية في التعامل مع البيانات**: تمثل السرية المتطلب الأمني الأكثر وضوحًا الذي يجب تلبيته. ويمكن أن يكفل التشفير سرية البيانات، ومع ذلك يجب أن تحترم آليات المزامنة اللازمة لدفع البيانات بكفاءة في السحابة التعديلات بطريقة مشفرة. وذلك بناءً على خوارزميات التفاضل، كما أن نقل البينات بين نسختين (مستخدمين) يقلل من احتمال تسرب البيانات. إن عدم التعامل بحذر كافٍ يؤدي إلى زيادة عبء المزامنة بشكل غير مستدام. وهكذا، تتمتع التقنيات بقدرتها على خفض حجم البيانات عن القيام بالمزامنة، وهذا يحسن من الكفاءة، ويقلل من نفاذ الموارد. وبذلك، يمكن تحقيق توازن بين الأمان والأداء في التخزين السحابي، مما يضمن حماية البيانات بشكل فعال مع الحفاظ على سرعة وكفاءة الوصول إليها[١].

من أجل زيادة الوعي بالبيانات، يجب إنشاء إدارة مفاتيح مناسبة لتوفير مشاركة آمنة للبيانات. ونظرًا لأن المشاركة والتعاون يمثلان حالات استخدام رئيسية لتخزين السحابة، فلا ينبغي إعاقة هذه الوظيفة. وبالتالي فإن الوعي بالسرية في السحابة ليس مجرد مسألة تشفير، بل يتطلب أيضًا مزامنة وإدارة مفاتيح تعتمد على التشفير، وهذا يساعد في التعامل الفعّال مع البيانات المشفرة[٢].

(1) Sambaiah. G, E. Kiran Kumar. (2020). Imperative Requirements for Data Security in Cloud Computing. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Vol 9. Iss 7. https://doi.org/10.17577/ijertv9is070455.

(2) Singh, U., Tiwari, A., & Sharma, S. (2023). DATA SECURITY IN CLOUD COMPUTING. journalofcardiovasculardiseaseresearch. Vol 12. Iss 2. PP 696 – 705. https://doi.org/10.48047/jcdr.2021.12.02.91.

٢- **الحفاظ على البيانات المتاحة**: إلى جانب الحاجة إلى الحفاظ على السرية دون تقليل الوظائف القائمة على السحابة، هناك ضمانات لاستمرار توفر البيانات المخزنة في السحابة بشكل دائم. إذ تؤدي الاتاحة العالية لخدمات السحابة إلى الاعتقاد بأن البيانات المخزنة في السحابة ستظل متاحة دائمًا، ونتيجة لذلك، غالبًا ما لا يقوم المستخدمون بعمل نسخ احتياطية لبياناتهم عند دفعها إلى السحابة(١).

ومع ذلك، قد تحدث الأخطاء في البنى التحتية السحابية. بالإضافة إلى الاضطرابات داخل البنية التحتية للسحابة نفسها، إذ يمثل عنق زجاجة في التعامل مع البيانات، والذي يتعلق بمعدلات نقل البيانات بطيئة ناتجة عن خلل في إحدى التقنيات المستخدمة، وأيضًا يعكس نقطة ضعف تتعلق بالوصول(٢).

وتوفر الأساليب الحالية تكرار البيانات من خلال تخزينها على عدة سحابات، مثل نموذج السحابة المجمعة DepSky. إلى جانب استخدام عدة سحابات، توفر التخزين المحلي المؤقت للبيانات حلاً ممكنًا لمواجهة اضطرابات الشبكة(٣).

(1) Celesti A., Fazio M., Villari M. & Puliafito A. (2016). Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems. Journal of Network and Computer Applications. Vol 59. PP 208 - 218. https://doi.org/10.1016/j.jnca.2014.09.021.

(2) Abadi A. (2022). Smarter Data Availability Checks in the Cloud: Proof of Storage via Blockchain. In M. Wynn (Ed.), Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies. IGI Global Scientific Publishing. PP 320 - 339. https://doi.org/10.4018/978-1-7998-7712-7.ch017

(3) Ibid. PP 320 - 339

ويتطلب ضمان الأمان والمرونة في التخزين السحابي النظر إلى مختلف التحديات والتقنيات المتاحة. ومن خلال تحقيق توازن بين السرية العالية، الاتاحة المستمرة، وتكرار البيانات، يمكن توفير بيئة تخزين سحابية آمنة وفعالة تلبي احتياجات المستخدمين وتحافظ على بياناتهم بأمان.

٣- **التحقق من اتساق البيانات**: نظرًا لفقدان السيطرة الفعلية، تصبح الفحوصات ضرورية للوعي بحالة البيانات، وبناءً على التخزين المؤقت المحلي الجزئي للبيانات، يمكن استخدام فحوصات السلامة الجاهزة مثل التي توفرها Amazon، على الرغم من أن الغرض الرئيسي من تلك الفحوصات هو الوعي بأخطاء النقل(١).

ولذلك فإن إتباع نهج مثل HAIL قد يعمل على سد هذه الفجوة استنادًا إلى التكرار والتحقق من الكتل باستخدام التوقيعات والمجاميع الاختبارية. ونظرًا لأن السحابة ساكنة، وتبقى تحت السيطرة الفنية لمزود الخدمة، فإن فحوصات السلامة في السحابة تعتمد على الثقة في مزود الخدمة، مما يستدعي الحاجة إلى وضع لوائح مناسبة بين العميل ومزود الخدمة(٢).

(1) B. Li, Q. He, F. Chen, H. Jin, Y. Xiang and Y. Yang. (2021). Auditing Cache Data Integrity in the Edge Computing Environment. in IEEE Transactions on Parallel and Distributed Systems. Vol 32. Iss 5. PP 1210 – 1223. doi: 10.1109/TPDS.2020.3043755.

(2) Zhao Y., Qu Y., Xiang Y. & Gao L. (2022). A Comprehensive Survey on Edge Data Integrity Verification: Fundamentals and Future Trends. ArXiv, abs/2210.10978. https://doi.org/10.48550/arXiv.2210.10978.

أن هذا النهج يعزز من التحقق من سلامة البيانات واتساقها، مما يضمن تقديم خدمة سحابية موثوقة وآمنة للمستخدمين. وتبني هذه الحلول يمكن أن يساهم في زيادة الثقة بين العملاء ومزودي الخدمة.

٤- **تتبع العمليات على البيانات**: تشير المسؤولية إلى إمكانية رصد العمليات المنفذة على عناصر معينة ضمن البيانات. حيث تمثل عمليات التسجيل والتدقيق، بالإضافة إلى إنشاء السياسات واللوائح للوصول، وذلك لضمان أن يمون هناك نهجًا مباشرًا لضمان المساءلة(١).

ونظرًا لأننا نعتمد فقط على تخزين البيانات، فإن استخدام إصدارات متقدمة من البيانات يعد آلية مباشرة لضمان المساءلة. كما يجب أن تكون مثل هذه الإصدارات مقاومة للتلف الذي قد يصيب النسخ الفردية لضمان سهولة إعادة بناء أي نسخة. نظرًا لبُعد البيانات عن موقع التخزين، يجب أن تكون التعديلات المتتابعة متوازنة وملائمة للتشفير لضمان عملية نقل فعالة(٢).

فعملية تتبع العمليات على البيانات تعد جانبًا حيويًا لضمان المساءلة والأمان في التخزين السحابي. ومن خلال استخدام تقنيات التسجيل والتدقيق، بالإضافة إلى إدارة الإصدارات المتقدمة من البيانات، يمكن تحقيق مستوى عالٍ من الشفافية والسيطرة على البيانات.

---

(1) Yang Z., Wang W. & Huang Y. (2017). Ensuring reliable logging for data accountability in untrusted cloud storage. 2017 IEEE International Conference on Communications (ICC). PP 1 - 6. https://doi.org/10.1109/ICC.2017.7997109.

(2) Wiegand E., Liu A. & Sedovic S. (2024). Algorithmic Accountability for Record Linkage. International Journal of Population Data Science. Vol 9. Iss 5. doi: 10.23889/ijpds.v9i5.2854.

٥- **تحقيق الأمان في التخزين السحابي**: انتهاك أي متطلب أمني يؤدي إلى ضعف في تخزين السحابة. ولذلك، يجب تطبيق السرية، والاتاحة، والسلامة، والمسؤولية بشكل متزامن لتحقيق الضمان. فبعض هذه التقنيات تلبي أكثر من متطلب أمني واحد. إذ تضمن أكواد للمحو وتتيح داخل DepSky وتحافظ على سلامة البيانات باستخدام الحسابات التي تعتمد عليها. وعند دمجها مع إصدار البيانات، يمكن تحقيق أهداف أمان أعلى مثل عدم الإنكار(١).

ونظرًا لأن الإجراءات يمكن تطبيقها فقط على جانب العميل من عتبة السيطرة الفنية، تصبح الإجراءات التي تضمن تخزين الآمن للمعلومات على جانب مزود الخدمة السحابية ضرورية لتوفير ضمان شامل.

ولذلك يجب تحقيق التوازن بين السرية، والاتاحة، والسلامة، والمسؤولية في التخزين السحابي لضمان تقديم خدماته. وبفضل تكامل الإجراءات الفنية والقانونية، يمكن تحقيق مستوى عالٍ من الأمان يلبي احتياجات المستخدمين، ويوفر حماية فعالة للبيانات.

٢,٢. الأبعاد القانونية للتخزين السحابي:

التخزين السحابي، فعلى الرغم من مزاياه التقنية العديدة، يخضع لعدة أبعاد قانونية. فيما يلي أهم الأبعاد القانونية للتخزين السحابي:

(1) P. Yang N. Xiong & J. Ren. Data Security and Privacy Protection for Cloud Storage: A Survey. in IEEE Access. Vol 8. PP 131723 - 131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

١- **الالتزام بحماية البيانات والخصوصية**: عالمية خدمات السحابة تثير تساؤلات حول ملكية البيانات، وحقوق الوصول إليها، والالتزام بالمعايير القانونية، والتي قد تختلف من دولة لأخرى، وهذه القوانين تفرض متطلبات لحماية بيانات المستخدمين وضمان خصوصيتهم. ولذلك، يتعين على مقدمي الخدمات السحابية الالتزام بمجموعة واسعة من القوانين واللوائح، لضمان الامتثال وتقديم خدمات موثوقة وآمنة(١).

ينبغي لمزودي الخدمة الحصول على موافقة المستخدمين قبل جمع بياناتهم أو معالجتها. فالموافقة يجب أن تكون واضحة وصريحة لضمان احترام حقوق الخصوصية للمستخدمين(٢).

وتشمل حقوق المستخدمين الحق في الوصول إلى بياناتهم، تعديلها، أو حذفها. وهذه الحقوق تمكن المستخدمين من السيطرة على بياناتهم وضمان استخدامها بطرق تتوافق مع رغباتهم وتوقعاتهم(٣).

(1) Mamanazarov S. (2023). DATA OWNERSHIP RIGHTS: FEASIBLE? LEGAL AND TECHNICAL SOLUTIONS. Tsul legal report. https://doi.org/10.51788/tsul.lr.4.4./gvtj6320.

(2) Dreyer J., Heitmann S., Erdmann F., Bauer G. & Kray C. (2022). 'Informed' consent in popular location based services and digital sovereignty. Journal of Location Based Services. Vol 16. Iss 4. PP 312 - 342. https://doi.org/10.1080/17489725.2021.2017495.

(3) Robol M., Breaux T., Paja E. & Giorgini P. (2022). Consent Verification Monitoring. ACM Transactions on Software Engineering and Methodology. Vol 32. Iss 1. PP 1 - 33. https://doi.org/10.1145/3490754.

إن الالتزام بالقوانين يعد أمرًا هامًا لضمان توفير خدمات التخزين الآمنة والفعالة. ومن خلال احترام الأنظمة والقوانين، يمكن لمزودي الخدمات بناء ثقة قوية مع العملاء وحماية بياناتهم بشكل فعّال.

٢- **السيادة على البيانات**: العديد من القوانين الوطنية تشترط تخزين البيانات داخل حدود الدولة لضمان السيادة على البيانات. فعلى سبيل المثال، تفرض قوانين الصين والهند تخزين البيانات محليًا لضمان أن تكون تحت السيطرة القانونية للدولة(١).

كما يتم تنظيم نقل البيانات بين الدول من أجل توافقها مع القوانين الداخلية. وهذه التنظيمات تهدف إلى حمايتها، وضمان العمل بمعايير الأمان والخصوصية العالمية(٢).

فالسيادة على البيانات تشكل معضلة مهمة، وتطلب التوافق مع القوانين الداخلية، إذ تختلف من دولة لأخرى. والامتثال يضمن حمايتها، مصداقية الخدمة المقدمة للمستخدمين في مختلف الدول.

٣- **المسؤولية القانونية**: الخدمات السحابية تنطوي على أخطار أمنية تشمل اختراق البيانات أو فقدانها. لذلك، وتُحدد الأبعاد القانونية تكون مسؤولية مزودي الخدمات في

(1) Меньшиков П.В. & Михина Л. К. (2022). Система противодействия угрозам информационной безопасности КНР// Вестник Забайкальского государственного университета. Т 28. № 1. PP 124 - 139. DOI: 10.21209/2227-9245-2022-28-1-124-139.

(2) Chaudhuri R. & Joseph, A. (2024). Living in a fragmented world: India's data way. India Review. Vol 23. Iss 2. PP 154 - 176. https://doi.org/10.1080/14736489.2024.2324638.

حالات الحوادث السيبرانية. وتشمل هذه المسؤولية تقديم تقارير فورية عن الحوادث وتعويض المستخدمين المتضررين[١].

فالعقود بين كلًا من مزودي الخدمة والمستخدمين[٢]، تضع حدود المسؤولية في حالات الفقدان أو الانتهاكات الأمنية. كما توضح العقود الجهات المسؤولة عند وقوع أي انتهاكات، وتضع إطارًا قانونيًا لحماية جميع الأطراف[١].

(1) Islam M. (2024). Protecting Data Access Liabilities in Cloud Computing. Journal of Artificial Intelligence General science (JAIGS). Vol 3. Iss 1. PP 180 -200. ISSN:3006-4023. https://doi.org/10.60087/jaigs. vol03. issue01. p195.

(٢) العقود هي حجر الزاوية في علاقة المستخدم بمزودي خدمات التخزين السحابي. وهذه العقود، التي غالبًا ما تكون أحادية الجانب، وفيها يفرض أحد الأطراف شروطًا لا يمكن التفاوض عليها، تحدد حقوق ومسؤوليات كل طرف وبالتالي يكون هذا العقد هو "عقد إذعان".

فعقود الإذعان هي عقود يتم فيها قبول الشروط الجاهزة من قبل الطرف الأضعف (المستخدم) دون إمكانية التفاوض عليها. وفي سياق التخزين السحابي، يقبل المستخدم شروط الخدمة التي يفرضها مزود الخدمة، والتي تحدد حقوقه وواجباته، وكذلك حدود مسؤولية مزود الخدمة. وتكمن أهمية عقود الإذعان في التخزين السحابي:

١- **حماية مزودي الخدمة**: تهدف هذه العقود إلى حماية مزودي الخدمات من المسؤولية عن أي ضرر قد يلحق بالمستخدمين نتيجة لاستخدام الخدمة.
٢- **توحيد الشروط**: تعمل هذه العقود على توحيد الشروط والمعايير المتعلقة بالخدمة، مما يسهل إدارة العلاقة بين مزود الخدمة والمستخدمين.
٣- **تحديد المسؤوليات**: تحدد العقود بوضوح مسؤولية كل طرف، مما يقلل من النزاعات القانونية.

ومن أبرز بنود عقود الإذعان في التخزين السحابي:

١- **حدود المسؤولية**: غالبًا ما تحدد العقود حدودًا لمسؤولية مزود الخدمة عن فقدان البيانات أو تلفها أو أي ضرر آخر قد يتعرض له المستخدم.
٢- **إخلاء المسؤولية**: قد تتضمن العقود بنودًا تخلي مزود الخدمة عن المسؤولية عن أي ضرر غير مباشر أو تبعي ناتج عن استخدام الخدمة.

=

وتلزم القوانين مزودي الخدمة بالإبلاغ عن أي خرق للبيانات فور حدوثه. وهذا الالتزام يضمن أن المستخدمين على علم بأي تهديدات لأمان بياناتهم، بحيث يمكنهم اتخاذ الإجراءات المناسبة لحماية معلوماتهم(٢).

إن المسؤولية القانونية تمثل جانبًا حيويًا من الأبعاد القانونية للتخزين السحابي. ومن خلال تحديد حدود المسؤولية وإشعار الانتهاكات، يمكن تحقيق حماية أكبر للبيانات وضمان التزام جميع الأطراف بالمعايير القانونية اللازمة.

٤- **الملكية الفكرية**: مع استعمال التخزين السحابي في مجالات بحثية أو تجارية، تكون حماية حقوق الملكية الفكرية أمرًا بالغ الأهمية. ويتطلب ذلك وجود قوانين تحمي البيانات الحساسة والمعلومات، والتي تُعد جزءًا من أصول الشركات. وهذه القوانين

=

٣- **تغيير الشروط**: يحفظ مزود الخدمة لنفسه الحق في تغيير شروط الخدمة في أي وقت، مما قد يؤثر على حقوق المستخدم.

٤- **فترة التخزين**: تحدد العقود المدة التي سيقوم فيها مزود الخدمة بتخزين البيانات، وقد تكون هذه المدة محدودة.

٥- **حقوق النسخ الاحتياطي**: يطلب مزود الخدمة من المستخدم القيام بإنشاء نسخ احتياطية من بياناته، مما يقلل من مسؤوليته في حالة فقدان البيانات.

عقود الإذعان تلعب دورًا حاسمًا في تنظيم علاقة المستخدمين بمزودي خدمات التخزين السحابي. ومع ذلك، يجب أن يتم النظر في هذه العقود بعناية، مع الأخذ في الاعتبار التوازن بين حماية حقوق المستخدمين وحماية مصالح مزودي الخدمة. ومن الضروري أن تتطور التشريعات لتواكب التطورات التكنولوجية، وأن يتم توعية المستخدمين بحقوقهم وواجباتهم.

(1) Montagnani M. & Cavallo M. (2018). Cybersecurity and Liability in a Big Data World. European Economics: Microeconomics & Industrial Organization eJournal. Vol 11. Iss 2. PP 71 – 99. https://doi.org/10.2139/ssrn.3220475.

(2) Zou Y. & Schaub F. (2019). Beyond Mandatory: Making Data Breach Notifications Useful for Consumers. IEEE Security & Privacy. Vol 17. Iss 2. PP 67 - 72. https://doi.org/10.1109/MSEC.2019.2897834.

تـضمن أن البيانـات البحثيـة والتجاريـة تبقـى آمنـة وغيـر معرضـة للاسـتخدام غيـر المصرح به[١].

إذ يجـب أن تظـل ملكيـة البيانـات بيـد المـستخدم، وعلـى مـزودي الخدمـة التأكـد مـن عـدم اسـتخدام البيانـات لأغـراض تجاريـة دون موافقـة صـريحة. وهـذا يـضمن حمايـة حقـوق المـستخدمين فـي بيانـاتهم الشخـصية والتجاريـة وعـدم اسـتغلالها بـدون إذن[٢].

كما يتعين على مزودي الخدمة احترام قوانين حقوق النشر وضمان عدم مشاركة المحتوى المحمي مع أطراف ثالثة. وهذه الإجراءات ضرورية للحفاظ على الملكية الفكرية وضمان عدم استخدام أو توزيع المحتوى المحمي بشكل غير قانوني[٣].

٥- **الامتثـال التنظيمـي للقـوانين والاتفاقيـات الدوليـة**: القـوانين المعنيـة بحمايـة البيانـات تـشكل تحـديًا كبيـرًا فـي عمليـات التخـزين الخـاص بالمعلومـات والبيانـات داخـل السحابات الالكترونية، خاصـة مـع وجـود اختلافـات قانونيـة بـين الـدول. فعلـى سـبيل

(1) Wang Y. (2021). Security-driven distributed platforms for intellectual property resource provision - a case study of TSITE IP. J Cloud Comp. Vol 10. Iss 56. https://doi.org/10.1186/s13677-021-00274-2.

(2) Zhang W. & Zhang Y. (2023). Enigma of Relationship between Digital Economy and Intellectual Property Rights: Reflections on Innovation in Digital Economy Represented by Cloud Computing. EAI Endorsed Transactions on Scalable Information Systems. Vol 10. Iss 6. https://doi.org/10.4108/eetsis.3946.

(3) Yang P., Xiong N. & Ren J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access. Vol 8. PP 131723 - 131740. https://doi.org/10.1109/ACCESS.2020.3009876.

المثال، قد يتطلب القانون في دولة معينة تخزين البيانات داخل حدودها الجغرافية، مما يؤثر على مزودي الخدمات السحابية العاملين عبر الحدود(١).

وقد تطلب بعض النظم امتثال مزود خدمة التخزين السحابي لمعايير معين، مثل ISO 27001 لضمان الأمان، و2 SOC لتقييم الضوابط الأمنية. وهذه المعايير تساعد في ضمان أن مزودي الخدمات السحابية يتبعون أفضل الطرق في حفظ البيانات وتأمينها(٢).

وعلى مزودي الخدمة إصدار تقارير منتظمة تبين كيفية معالجة البيانات. وهذا من شأنه أن يعزز من مستوى الشفافية والثقة بين المستخدمين ومزودي الخدمات، ويتيح لهم الاطلاع على السياسات والإجراءات المتبعة في وقاية بياناتهم(٣).

٦- **قوانين الحماية من الجرائم السيبرانية**: الخدمات السحابية تنطوي على أخطار أمنية تشمل اختراق البيانات أو فقدانها. لذلك، تُحدد الأبعاد القانونية مسؤولية مزودي الخدمات في حالات الحوادث السيبرانية. وتشمل هذه المسؤولية تقديم تقارير فورية عن الحوادث وتعويض المستخدمين المتضررين(٤).

---

(1) Bakare S., Adeniyi A., Akpuokwe C. & Eneh N. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. Computer Science & IT Research Journal. Vol 5. Iss 3. PP 528 - 543. https://doi.org/10.51594/csitrj.v5i3.859.

(2) Kitsios F., Chatzidimitriou E. & Kamariotou M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability. Vol 15. 5828. https://doi.org/10.3390/su15075828.

(3) Awasthi M. (2022). Verifiable and Practical Compliance for Data Privacy Laws. 2022 IEEE 29th International Conference on High Performance Computing, Data and Analytics Workshop (HiPCW). PP 59-60. https://doi.org/10.1109/HiPCW57629.2022.00013.

(4) Dharmawan, N., Kasih, D., & Stiawan, D. (2019). Personal data protection and liability of internet service provider: a comparative approach. =

إذ يجب أن تكون البنية التحتية للتخزين السحابي محمية من الهجمات السيبرانية وفقًا للقوانين الدولية والمحلية. وهذا يتطلب تطبيق إجراءات أمان صارمة لضمان حماية البيانات من أي تهديدات سيبرانية(١).

كما يجب على مزودي الخدمة التعاون مع السلطات في تقديم الأدلة الرقمية، بشرط الالتزام بقوانين الخصوصية. وهذا التعاون يساهم في التحقيقات السيبرانية ويعزز من تطبيق العدالة، مع الحفاظ على حقوق الخصوصية للمستخدمين(٢).

٧- **حفظ واسترجاع البيانات**: إذ يجب تحديد المدة التي ستظل البيانات مخزنة فيها وما إذا كانت هناك خيارات لاسترجاعها بعد الحذف. وهذا يشمل وضع جهود واضحة للتعامل مع البيانات، وضمان توفر خيارات لاسترجاع البيانات عند الحاجة حتى بعد الحذف(٣).

كما يجب أن تمنح القوانين للمستخدمين الحق في حذف بياناتهم نهائيًا من أنظمة التخزين السحابي (الحق في النسيان). وهذا الحق يضمن للمستخدمين القدرة على

=

International Journal of Electrical and Computer Engineering (IJECE). Vol 9. Iss 4. PP 3175 – 3184. https://doi.org/10.11591/IJECE.V9I4.PP3175-3184.

(1) Montagnani M. & Cavallo M. (2018). Cybersecurity and Liability in a Big Data World. Op. cit PP 71 – 99

(2) Dye O., Heo J. & Cankaya E. (2024). Reflection of Federal Data Protection Standards on Cloud Governance. ArXiv, abs/2403.07907. https://doi.org/10.5121/csit.2024.140424.

(3) Nachiappan R., Calheiros R., Matawie K. & Javadi B. (2023). Optimized Proactive Recovery in Erasure-Coded Cloud Storage Systems. IEEE Access. Vol 11. PP 38226 - 38239. https://doi.org/10.1109/ACCESS.2023.3267106.

إزالة بياناتهم بالكامل من السحابة وعدم ترك أي أثر لها، بما يتوافق مع قوانين حماية البيانات والخصوصية[١].

فالحفظ والاسترجاع في التخزين السحابي يتطلب وضع سياسات واضحة ودقيقة لضمان تخزين البيانات على المدى الطويل وإتاحة خيارات لاسترجاعها. بالإضافة إلى ذلك، يتيح حق النسيان للمستخدمين القدرة على التحكم الكامل في بياناتهم وحذفها بشكل نهائي عند الحاجة. وتحقيق هذا التوازن يساهم في تقديم خدمات تخزين سحابية موثوقة وآمنة[٢].

٨- **حوكمة البيانات والشفافية**: يجب أن يلتزم مزودو الخدمات السحابية بممارسات شفافة توضح للمستخدمين مواقع تخزين بياناتهم. وهذا يساعد في تعزيز الشفافية والثقة، حيث يعرف المستخدمون مكان تخزين بياناتهم وكيفية التعامل معها[٣].

وعلى مزودي الخدمة أيضًا توضيح كيفية معالجة البيانات وما هي الإجراءات المتبعة لحمايتها. وهذا يشمل تقديم معلومات حول تقنيات التشفير، إجراءات النسخ الاحتياطي، ومراقبة الوصول لضمان أمان البيانات[١].

---

(1) Susi M. (2020). The Right to Be Forgotten. In A. von Arnauld K. von der Decken & M. Susi (Eds.), The Cambridge Handbook of New Human Rights: Recognition. Novelty. Rhetoric. Chapter. Cambridge: Cambridge University Press. PP 287 – 299. https://doi.org/10.1017/9781108676106. 023.

(2) Д. М. Бєлов, М. В. Бєлова & О. Т. Горнило. (2024). Право людини на забуття. Науковий вісник Ужгородського національного університету. Серія: Право. Том 2 № 81. PP 57 – 63. https://doi.org/10.24144/2307-3322.2024.81.2.9.

(3) Yu. S. Kharitonova. (2023). Legal Means of Providing the Principle of Transparency of the Artificial Intelligence. Journal of Digital Technologies and Law. Vol 1. Iss 2. PP 337 – 358. https://doi.org/10.21202/jdtl.2023.14.

كما يتعين على مزودي الخدمات السحابية الإفصاح عن الأطراف التي يمكنها الوصول إلى بيانات المستخدمين. وهذا يشمل تقديم تفاصيل حول الشركاء والمقاولين الفرعيين الذين قد يكون لهم حق الوصول إلى البيانات في إطار تقديم الخدمات[٢].

ومن خلال الالتزام بالمنهجية السابقة، يمكن لمزودي الخدمات بناء الثقة بين المستخدمين ومزودي الخدمات. وهذه الممارسات تساهم في بناء علاقات متينة وموثوقة، وتضمن تقديم خدمات سحابية آمنة وفعالة تلبي توقعات المستخدمين.

الجوانب القانونية للتخزين السحابي تهدف إلى حفظ البيانات، وضمان الحقوق، وتعزيز الثقة بين مقدمي الخدمات والعملاء. فالقوانين واللوائح المحلية والدولية أمر ضروري لتجنب النزاعات القانونية وضمان الامتثال. ومن خلال الالتزام بها، يمكن لمقدمي الخدمات تقديم حلول تخزين آمنة وموثوقة تلبي احتياجات المستخدمين، مع حماية حقوق الخصوصية، وسرية البيانات الحساسة. هذا التوازن يساعد على بناء علاقات طويلة الأمد قائمة على الثقة والمصداقية بين جميع الأطراف.

التطور التاريخي للتشريعات المتعلقة بالتخزين السحابي:

شهدت التشريعات المتعلقة بالتخزين السحابي تطورًا ملحوظًا على مدى العقود الماضية، مدفوعة بتسارع تبني التكنولوجيا الرقمية وزيادة الاعتماد على الحلول السحابية. وهذا التطور في الإطار القانوني كان استجابة للحاجة إلى تنظيم استخدام البيانات في بيئات سحابية معقدة.

=

(1) Truong N., Sun K., Lee G. & Guo Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security. Vol 15. https://doi.org/10.1109/TIFS.2019.2948287.

(2) Dye O., Heo J. & Cankaya E. (2024). Reflection of Federal Data Protection Standards on Cloud Governance. ArXiv. Op. cit.

ففي البدايات، كانت التشريعات بسيطة نسبيًا وتركز على حماية البيانات من الضياع أو الاختراق. ولم يكن هناك تركيز كبير على الجوانب القانونية، أو التنسيق بين الدول في هذا الصدد. مع زيادة الاعتماد على التخزين السحابي في الأغراض التجارية والشخصية، بدأت الدول في تطوير قوانين أكثر تعقيدًا. وأهم هذه القوانين كانت "اللائحة العامة لحماية البيانات (GDPR)" للاتحاد الأوروبي، فقد وضعت معايير صارمة لحفظ البيانات الشخصية، وحمايتها، وتبادلها بين الدول[١].

ونهض التخزين السحابي بشكل هائل خلال العقود الماضية، مما أدى إلى تغييرات جذرية في طريقة تخزيننا ومعالجتنا للبيانات. وبالتزامن مع هذا التطور، شهدنا أيضًا تطورًا ملحوظًا في التشريعات التي تحكم هذا المجال الحيوي. وتتبع هذا التطور يعكس أهمية مواكبة التغيرات التكنولوجية والإطار القانوني لضمان البيانات وحمايتها، وحقوق المستخدمين. يمكن تقسيم هذا التطور إلى مراحل رئيسية:

١- **المرحلة التمهيدية: البدايات (١٩٩٠ –٢٠٠٠):** وفيها، لم تكن هناك تشريعات مخصصة للتخزين السحابي. وبدلًا من ذلك، كانت القوانين القائمة المتعلقة بالبيانات بصفة عامة، والتجارة الإلكترونية هي المرجع الرئيسي لضبط هذا المجال[٢].

(1) Dimitrova Diana. (2021). THE NEW STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA BETWEEN EU AND NON-EU COUNTRIES. PROTECTION OF THE PERSONAL DATA AND THE DIGITALIZATION - CHALLENGES AND PERSPECTIVES 2021 CONFERENCE PROCEEDINGS. PP 106 - 115. https://doi.org/10.36997/ppdd2021.106.

(2) Matana, T. (2024). Origin & History of ASP SaaS, PaaS and Cloud Computing. International Journal of Scientific Research and Management =

فالولايات المتحدة الأمريكية كان قانون الخصوصية الفيدرالي لعام ١٩٧٤ (Privacy Act of 1974) واحدًا من القوانين المعتمدة، والتي تحكم البيانات الشخصية وحمايتها[١]. أما الاتحاد الأوروبي فكان هناك توجيه "حماية البيانات الأوروبي" لعام ١٩٩٥ (EU Data Protection Directive 1995)، وكان إطارًا قانونيًا هامًا يهدف إلى حماية البيانات، وضمان استخدامها[٢].

وهذه المرحلة شهدت الدول العربية غياب تشريعات محددة، شأنها شأن العديد من الدول، كما عانت الدول العربية في البداية من غياب تشريعات خاصة تحكم التخزين السحابي. وقد اعتماد على التشريعات الموجودة المتعلقة البيانات بصفة عامة، وحقوق الملكية الفكرية، وكان يتم تطبيقها على هذا المجال الجديد، ولكنها لم تكن كافية.

=

(IJSRM). Vol 12. Iss 10. PP 1571 - 1607. https://doi.org/10.18535/ijsrm/v12i10.ec08.

(1) Privacy Act. (N. D.). The Privacy Act of 1974, as amended, provides safeguards against unwarranted invasions of privacy by establishing a code of "fair information practices". U.S. Department of the Treasury. Available through the following link: https://home.treasury.gov/footer/privacy-act. It was viewed on: 25/12/2024.

(2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Official Journal L 281, 23/11/1995 P. 0031 – 0050. An official website of the European Union. Available through the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. It was viewed on: 25/12/2024.

وركزت هذه القوانين على التعامل مع البيانات الشخصية، وحيتها، وضمان سريتها وأمنها، خاصة في البيئات الالكترونية. وهذه الفترة شكلت الأساس لوضع قوانين مستقبلية وخاصة للحوسبة السحابية.

فهذه المرحلة شهدت بداية التقنيات السحابية، دون وجود تشريعات خاصة بها، مما أدى إلى الاعتماد على القوانين الموجودة مسبقًا في التعامل مع حفظ البيانات وحمايتها. وهذه القوانين شكلت الأساس لتطوير إطار قانوني أقوى وأكثر تخصصًا في الفترات اللاحقة.

٢- **المرحلة الانتقالية: ظهور النظم القانونية (٢٠٠٠ - ٢٠١٠):** مع تقدم تقنيات الحوسبة السحابية وانتشار استخدام الإنترنت، بدأت الدول والمؤسسات الدولية في إدراك الحاجة إلى تنظيم هذه التقنيات. حيث قد أصبحت الحوسبة السحابية أداة حيوية للشركات والأفراد، مما دفع الجهات المعنية إلى وضع نظم قانونية تنظمها.

وقد شهدت هذه المرحلة صدور قوانين تضمنت أحكامًا تتعلق بحماية البيانات والتعامل مع البيانات العابرة للحدود. وأحد الأمثلة البارزة هو "قانون الالتزام بحماية البيانات الصحية (HIPAA)" في الولايات المتحدة الامريكية، الذي شدد على حماية البيانات الصحية، وخاصة الإلكترونية، مع ضمان سريتها وأمنها[1].

(1) Andriole, K. (2014). Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology (JACR). Vol 11. Iss 12. PP 1212 - 1216. https://doi.org/10.1016/j.jacr.2014.09.011.

ومن ثم؛ بدأت الدول في وضع قوانين تتعلق بنقل البيانات، لضمان حمايتها، وفقًا للقوانين الخاصة بكل منها. وهذه الخطوة كانت ضرورية لمواكبة التوسع في التقنيات السحابية وتوفير حماية كافية للبيانات في البيئات متعددة الجنسيات.

وفي الدول العربية كان الاعتماد على التخزين السحابي محدودًا للغاية، ومعظم القوانين المتعلقة بها تركز على الجرائم الإلكترونية، والتجارة الإلكترونية، ولم تكن هناك قوانين تنظم خدمات تلك التقنيات.

وشهدت هذه المرحلة تقدم كبير في الجوانب القانونية التي تنظمها. فمن خلال صدور قوانين جديدة وتنظيم نقل البيانات عبر الحدود، تمكنت الدول من توفير حماية أفضل، وضمان استخدامها بشكل مسؤول وآمن.

٣- **المرحلة الحالية: التشريعات المتقدمة (٢٠١٠ – الآن)**: مع انتشار التخزين السحابي بشكل واسع، تم وضع أطر قانونية أكثر تفصيلًا وتنظيمًا. ومن أبرز هذه الأطر:

١- **اللائحة العامة لحماية البيانات (GDPR):** "اللائحة العامة لحماية البيانات " قد دخلت حيز التنفيذ عام ٢٠١٨، ووضعت ضوابط صارمة تتعلق بحماية البيانات الشخصية. وفرضت التزامات على الشركات التي تقوم بجمع البيانات، معالجتها، مع التركيز على الخصوصية والتحكم وسهولة التحكم في البيانات[1].

(1) What is GDPR, the EU's new data protection law? (N. D.). GDPR.EU. Available through the following link: https://gdpr.eu/what-is-gdpr/. It was viewed on: 25/12/2024.

٢- **الولايات المتحدة:** أحد أبرز القوانين في هذا المجال هو قانون "خصوصية المستهلك في كاليفورنيا (CCPA)"، والذي بدأ تطبيقه عام ٢٠٢٠. ويهدف CCPA إلى تعزيز حقوق الخصوصية للمستهلكين، ويمنحهم الحق في معرفة البيانات التي يتم جمعها عنهم، حق طلب حذفها، وحق الاعتراض على بيعها[١].

٣- **الدول العربية:** أصدرت الامارات قوانين تعزز حماية البيانات الشخصية، مثل قانون حماية البيانات (٢٠٢٠)[٢]، والذي يشمل استخدام السحابة. ووضعت المملكة العربية السعودية سياسات خاصة بسيادة البيانات الوطنية في إطار رؤية (٢٠٣٠)، مثل متطلبات تخزين البيانات داخلها[٣]. وفي مصر أصدر "قانون حماية البيانات الشخصية" لعام (٢٠٢٠)[٤]. وقطر هناك قانون "حماية

(1) California Consumer Privacy Act (CCPA). (2024). State of California Department of Justice. Available through the following link https://oag.ca.gov/privacy/ccpa. It was viewed on: 25/12/2024.

(٢) القانون الاتحادي لحماية البيانات الشخصية. (٢٠٢٤). قوانين حماية البيانات. البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة. ومتاح من خلال الرابط التالي: https://u.ae/ar-ae/about-the-uae/digital-uae/data/data-protection-laws. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

(٣) سياسة الخصوصية. (ب. ت.). رؤية السعودية ٢٠٣٠. ومتاح من خلال الرابط التالي: https://www.vision2030.gov.sa/ar/annual-reports. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

(٤) في أغسطس ٢٠٢٠، تم إصدار رقم ١٥١ لسنة ٢٠٢٠، والمعروف باسم قانون حماية البيانات الشخصية، وقد تم نشره في الجريدة الرسمية ويتكون من ٤٩ مادة. القانون يهدف إلى تنظيم جمع ومعالجة البيانات الشخصية إلكترونيًا، سواء جزئيًا أو كليًا، للأشخاص الطبيعيين. وهو يحدد حقوق المواطنين في الحفاظ على خصوصيتهم ويضع معايير للشركات والجهات التي تتعامل مع البيانات الشخصية.

خصوصية البيانات" لعام (٢٠١٦)، مع تعديلات لاحقة لتعزيز دور التخزين السحابي.

وفي الكويت، وبالرغم من أن التشريعات المتعلقة بالتخزين السحابي ليست شاملة بعد، إلا أنها تتضمن قوانين وسياسات تهدف إلى حماية البيانات، مع حماية الخصوصية. فيما يلي أهم الجوانب المتعلقة بالتشريعات الكويتية:

- **حماية البيانات الشخصية والخصوصية**: شكل القانون رقم ٢٠ لسنة ٢٠١٤ بشأن الجرائم الإلكترونية، والذي يهدف إلى مكافحة الجرائم الرقمية أو الالكترونية، وحماية البيانات الشخصية، خاصة من الوصول غير المصرح به. كما يلزم القائمين على البيانات باتخاذ الاجراءات اللازمة لحمايتها وضمان خصوصية الأفراد(١).
- **الهيئة العامة للاتصالات وتقنية المعلومات "الجهة المنظمة"**: إذ تقدم الهيئة في الكويت دورًا محوريًا في تنظيم مجال الاتصالات وتقنية المعلومات، بما فيها خدمات التخزين السحابي. كما تقوم الهيئة بوضع الأنظمة واللوائح التي تحكم هذا القطاع، وتصدر التراخيص لمزودي الخدمات، وتراقب الامتثال لهذه اللوائح(٢).

(١) قانون رقم ٢٠ لسنة ٢٠١٤. (٢٠١٤). قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية. مجلس الوزراء – الجهاز المركزي لتكنولوجيا المعلومات. ومتاح من خلال الرابط التالي: https://www.e.gov.kw/sites/kgoArabic/Forms/MagazineA.pdf. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

(٢) الهيئة العامة للاتصالات وتقنية المعلومات. ومتاح من خلال الرابط التالي: https://citra.gov.kw/sites/Ar/Pages/AboutUs.aspx. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

إذ تشهد الكويت تطورًا تدريجيًا في التشريعات المتعلقة بالتخزين السحابي، حيث الاهتمام بحماية البيانات والأمن السيبراني. ومع ذلك، هناك حاجة إلى وضع قانون متخصص لحماية البيانات الشخصية، وتنظيم التخزين السحابي بشكل أكثر شمولية، مما يدعم التحول الرقمي في البلاد. بما يتماشى مع رؤية "كويت جديدة ٢٠٣٥"

فوضع تشريعات للتخزين السحابي يعكس التغيرات السريعة، والاحتياجات المجتمعية لحماية البيانات وتأمينها. ومع تقدم التقنيات الرقمية، وتصاعد الاعتماد على الحلول السحابية، تظهر الحاجة لوضع نظم قانونية تواكب هذه التحولات.

مع كل تطور تكنولوجي جديد، تظهر تحديات وفرص جديدة. فالتشريعات تعمل على معالجة تلك العقبات، من خلال وضع معايير وأطر قانونية تضمن حماية البيانات بفعالية. من المرجح أن تتوسع هذه التشريعات باستمرار لمواكبة تطورات العصر الرقمي. خاصة مع اعتماد المزيد من الكيانات على الحلول السحابية، ستزداد الحاجة إلى وضع قوانين ولوائح تضمن أمان البيانات وتعزز الثقة بين المستخدمين ومزودي الخدمات.

التنظيم القانوني للتخزين السحابي:

في ضوء التقدم السريع للتقنيات الرقمية، والاعتماد على التخزين السحابي، أصبح التنظيم القانوني لهذه التكنولوجيا ضرورة ملحة لكفالة حماية البيانات، وحقوق العملاء. ففي الدول الأوربية، تمثل "اللائحة العامة لحماية البيانات (GDPR)" تشريعًا متقدمًا، حيث تضع معايير صارمة لحماية البيانات الشخصية وخصوصية المستخدمين مع توفير سياق قانوني شامل.

أما في مصر، فقد خطت خطوات واضحة مع إصدار "قانون حماية البيانات الشخصية" لعام ٢٠٢٠، الذي يُلزم الكيانات بتطبيق معايير الأمان والخصوصية بما

يتماشى مع التوجهات الدولية. وفي الكويت، ورغم حداثة التشريعات، يُركز التنظيم القانوني على قوانين مثل "قانون الجرائم الإلكترونية" لعام ٢٠١٤، والذي يهدف إلى حماية البيانات من الانتهاكات وتعزيز الأمن السيبراني، مع وجود توجهات مستقبلية لوضع أطر شاملة. فهذه التشريعات تعكس تحديات مشتركة، وفرص متاحة لضمان استخدام آمن وفعال للتقنيات السحابية.

٤,١. التنظيم القانوني للتخزين السحابي من خلال "اللائحة العامة لحماية البيانات (GDPR)":

تُعتبر "اللائحة العامة لحماية البيانات (GDPR)" الصادرة عن الاتحاد الأوروبي عام ٢٠١٨ حجر الأساس في التعامل الالكتروني مع البيانات الشخصية[١]، بما

(١) تتميز اللائحة العامة لحماية البيانات بكونها لائحة قانونية مباشرة، مما يعني أنها تُطبق مباشرة على جميع الأطراف المستهدفة دون الحاجة إلى تحويلها إلى قوانين وطنية كما كان الحال مع التوجيه السابق. وأهداف اللائحة تشمل:

- **توحيد قواعد حماية البيانات**: لضمان اتباع معايير موحدة في جميع أنحاء الاتحاد الأوروبي.
- **تعزيز اليقين القانوني**: من خلال تقديم إطار قانوني واضح للشركات والأفراد.
- **تشجيع التدفق الحر للبيانات الشخصية**: عبر إزالة العقبات التي قد تعيق نقل البيانات داخل الاتحاد الأوروبي.
- **رفع مستوى الخصوصية للأفراد**: بتوفير حماية أكبر للبيانات الشخصية وتعزيز حقوق الأشخاص المتضررين.

وأصبحت تمثل نقلة نوعية في تنظيم حماية البيانات، حيث أصبحت معيارًا عالميًا يؤثر على الشركات والمؤسسات داخل الاتحاد وخارجه، مما يتطلب الامتثال من جميع الجهات التي تتعامل مع بيانات مواطني الاتحاد الأوروبي.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, =

فيها البيانات المخزنة عبر خدمات التخزين السحابي للبيانات. والهدف الرئيسي اللائحة هو حماية خصوصية الأفراد وتعزيز شفافية التعامل مع بياناتهم الشخصية، مما يضع إطارًا قانونيًا صارمًا لمقدمي الخدمات السحابية. وتؤثر اللائحة بشكل كبير على الإطار القانوني المحيط بالتخزين السحابي بصورة خاصة، مما يستلزم الامتثال من قبل مزودي الخدمات السحابية. وتؤكد هذه اللائحة على الخصوصية في التعامل مع البيانات، وتتطلب من الجهات القائمة عليها تنفيذ تدابير قوية لحمايتها(١).

في عام ٢٠٢١، اعتبرت المفوضية الأوروبية الحوسبة السحابية واحدة من المجالات الضعيفة التي تحتاج إلى تعزيز تنظيمي وتقني لضمان الامتثال، وحماية البيانات. واستجابة لذلك، تمت الموافقة على مدونتين لقواعد السلوك في مجال الحوسبة السحابية، وقد تم تطويرها بقيادة خبراء الصناعة، وبالتعاون مع الشركات المتخصصة في هذا المجال، وذلك بهدف تقديم استراتيجية عملية للامتثال "للائحة العامة لحماية البيانات (GDPR)"(٢).

=

GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV). available through the following link: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

(1) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. (2021). EUROPEAN COMMISSION. Available through the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206. It was viewed on: 27/12/2024.

(2) Luca Bertuzzi & Euractiv. (2021). Cloud development in Europe passes by GDPR compliance. Euractiv. available through the following link: https://www.euractiv.com/sections/tech/. visited on: 28/12/2024.

وتركز هاتين المدونتين على تأكيد الثقة في سوق الحوسبة السحابية داخل دول الاتحاد، وتشجيع التنافس بين مزودي تلك الخدمات من خلال إنشاء معايير موحدة تدعم الاذعان القانوني، وتحمي المستخدمين. وهذا التقدم يمثل خطوة مهمة نحو تنظيم بيئات الحوسبة السحابية، وتعزيزها كاختيار آمن وموثوق للمؤسسات والأفراد.

ويغطي الإطار التنظيمي لمدونات قواعد السلوك جانبين رئيسيين من الخدمة. هما:

١- **المدونة الأولى:** تحتوي على البرمجيات كخدمة (SaaS)، وتشمل مجموعة من مقدمي الخدمات البارزين مثل "Alibaba Cloud" و"Cisco" و"Dropbox" و"Google Cloud" و"Microsoft" و"IBM"، والذين يعملون على تحسين خدماتهم بما يتوافق مع "اللائحة العامة لحماية البيانات (GDPR)"[١].

٢- **المدونة الثانية:** تغطي البنية التحتية كخدمة (IaaS)، مع تميز Amazon Web Services (AWS) كمزود رئيسي في هذا المجال[٢].

وهؤلاء المزودون يعملون داخل سوق سحابية داخل الاتحاد الأوروبي، والذي يشهد نموًا مستمرًا، ما يجعل من الضروري لهم وللشركات الناشئة تحديث طرق للامتثال للائحة GDPR[١].

(1) Tsai W., Bai X. & Huang Y. (2014). Software-as-a-service (SaaS): perspectives and challenges. Science China Information Sciences. Vol 57. PP 1 - 15. https://doi.org/10.1007/s11432-013-5050-z.

(2) Metwally K., Jarray A. & Karmouch A. (2020). A Distributed Auction-based Framework for Scalable IaaS Provisioning in Geo-Data Centers. IEEE Transactions on Cloud Computing. Vol 8. Iss 3. PP 647 - 659. https://doi.org/10.1109/TCC.2018.2808531.

فعملية الامتثال تشكل "اللائحة العامة لحماية البيانات" عقبة كبيرة لكل من مقدمي الخدمات السحابية الكبار والناشئين، وفقًا لدراسة (Privacy-Aware Cloud Ecosystems and GDPR Compliance) والتي أجراها Barati & et al. قد أثرت هذه اللوائح الجديدة على حوكمة السحابة بشكل واسع. على سبيل المثال، وفقًا لتقرير Statista (٢٠٢٢)، حوالي ٦٣٪ من ممارسو أمن المعلومات في فرنسا يرون أن مؤسساتهم ستحتاج إلى تغييرات كبيرة في حوكمة السحابة لتتوافق مع متطلبات GDPR. وكانت النسب مشابهة في بلدان أخرى مثل ألمانيا الإتحادية (٥٧%) وبريطانيا (٥٦%)[٢].

وهذا التحول يعكس التأثير الواسع "اللائحة العامة لحماية البيانات" على الصناعة[٣]، ودفع هذا الجميع لاعتماد معايير عالية لحماية أمن البيانات ،وزيادة الشفافية في تقديم الخدمات السحابية.

=

(1) Soltani S., Martin P. & Elgazzar K. (2018). A hybrid approach to automatic IaaS service selection. Journal of Cloud Computing. Vol 7. Article number: 12. https://doi.org/10.1186/s13677-018-0113-8.

(2) M. Barati, O. Rana, G. Theodorakopoulos & P. Burnap. (2019). Privacy-Aware Cloud Ecosystems and GDPR Compliance. 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud). Istanbul. Turkey. PP 117- 124. https://doi.org/10.1109/FiCloud.2019.00024.

(٣) لتسهيل تكيف الشركات مع متطلبات الامتثال للائحة العامة لحماية البيانات، يتم الاعتماد على الهندسة الموجهة بالنموذج (MDE)، كما أوضحها كل من Davies. وMeliá. حيث يتمثل النهج في تعريف ملف تعريف خاص بـ لغة النمذجة الموحدة (UML) للهندسة المعمارية السحابية، مما يتيح تصميمًا يتوافق مع اللائحة GDPR من خلال تطوير قوالب نمطية مخصصة لهذا الغرض.

ويعتمد الاقتراح على تقنيات UML وملفات التعريف المرتبطة بها، وهي منهجيات شائعة في هندسة البرمجيات لتطوير الأنظمة. حيث تُستخدم القوالب النمطية لتحديد أنواع محددة للمجال من عناصر مخطط UML، مما يُمكّن المصمم من إنشاء كائنات UML ذات صلة مباشرة بمصطلحات

=

وتحدد تلك السياسة مجموعة من الشروط والقيود المتعلقة بالبيانات، والتي تصف كيفية التعامل مع البيانات أو نقلها بين الأطراف. فاستخدام السياسات يسمح بالتحكم الصارم في دورة حياة البيانات من أجل ضمان خصوصيتها وتطبيق لوائح محددة بشأن استخدام البيانات الشخصية والوصول إليها والإفصاح عنها(١).

ومن خلال السياسات الثابتة يتم تعزيز سيطرة مالكي البيانات على بياناتهم. وعلى وجه الخصوص، ترتبط السياسات القابلة للقراءة آليًا بالبيانات بشكل مباشر، وتُسمى ثابتة لأنها تنتقل مع البيانات أثناء انتقالها عبر نطاقات إدارية متعددة. وتتيح هذه

=

المشكلة المطروحة. على سبيل المثال، يمكن أن يكون الكائن "مُمثل" في مخطط حالة الاستخدام أو "مكوّن" في مخطط مكونات، مع سمات أو وظائف متخصصة مسبقًا وفقًا لمجال المشكلة. تستفيد هذه المنهجية من ملفات تعريف UML معروفة، مثل:

١- MARTE: مفيد لنمذجة الأنظمة المضمنة والوقت الحقيقي.

٢- DAM: يستخدم لتحليل سمات الاعتمادية.

٣- SecAM: مفيد لنمذجة وتحليل سمات الأمان.

ومن خلال تطبيق ملف تعريف UML مخصص للبيئات السحابية، يهدف هذا النهج إلى توفير أدوات قوية للمصممين لمواءمة تصميماتهم مع متطلبات GDPR، ما يعزز الامتثال التنظيمي والابتكار في تصميم الأنظمة السحابية.

Meliá S., Cachero C., Hermida J.M. et al. (2016). Comparison of a textual versus a graphical notation for the maintainability of MDE domain models: an empirical pilot study. Software Qual J Vol 24. PP 709 – 735. https://doi.org/10.1007/s11219-015-9299-x.

Jim D., Charles C., Edward C., David N. & Ib Holm S. (2005). Formality, Evolution, and Model-driven Software Engineering. Electronic Notes in Theoretical Computer Science. Volume 130. PP 39 – 55. ISSN 1571-0661. https://doi.org/10.1016/j.entcs.2005.03.004.

(1) S. Pearson & M. Casassa-Mont. (2011). Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer. Vol. 44. Iss 9. PP 60 - 68. https://doi.org/10.1109/MC.2011.225.

السياسات تنظيم كيفية الوصول إلى البيانات واستخدامها طوال دورة حياتها، مما يساعد على ضمان إمكانية تنفيذ قرارات التحكم في الوصول وتطبيقات السياسات بطريقة موزعة[1].

من خلال تلك السياسات يمكن لها أن تحدد من هو المالك الأصلي للبيانات، ومحتوها (التي قد تكون مشفرة)، والاستخدام الذي سيتم إجراؤه للبيانات (على سبيل المثال، للتحليل الإحصائي، ومعالجة المعاملات، والتسويق المستهدف)، ومن يمكنه الوصول إلى البيانات، والمدة القصوى للبيانات، بالإضافة إلى الالتزامات والقيود المحددة الأخرى للأطراف المعنية.

الركائز الأساسية لتنظيم التخزين السحابي بموجب "اللائحة العامة لحماية البيانات GDPR":

دخلت تلك حيز التنفيذ الفعلي في ٢٥ مايو ٢٠١٨، كخطوة مهمة لتوحيد قواعد حماية وحفظ البيانات بين دول الاتحاد. وتم اعتماد اللائحة في عام ٢٠١٦ لتحل محل توجيه حماية البيانات لعام ١٩٩٥، الذي كان يهدف إلى مواءمة معايير حماية البيانات داخل الاتحاد الأوروبي لتسهيل نقل البيانات بين الدول الأعضاء وعبر الحدود[2]. وتشمل الركائز الأساسية ما يلي:

١- **معالجة البيانات الشخصية بطريقة قانونية وشفافة**: إن الالتزام بمعالجة البيانات وخاصة الشخصية منها بطريقة قانونية وشفافة، هو أحد الركائز الأساسية في قوانين

(1) Ibid. PP 60 – 68.

(2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Op. cit.

حماية البيانات العامة. فمن خلال هذه المتطلبات تهدف اللائحة إلى تعزيز الثقة، مع ضمان أن البيانات الشخصية للأفراد يتم جمعها ومعالجتها، وفقًا لمعايير صارمة[١]. وذلك عن طريق:

- **الموافقة الواضحة والمسبقة**: ينبغي على مقدمي الخدمات السحابية إحراز موافقة صريحة من الأفراد قبل القيام بعملية جمع أو معالجة بياناتهم. كما ينبغي ان تكون تلك الموافقة قابلة للإثبات في أي وقت[٢].
- **الشفافية**: يجب إبلاغ المستخدمين بشكل واضح ومحدد عن كيفية استخدام بياناتهم والغرض من تخزينها. ويجب أن يكون هذا الإبلاغ بلغة بسيطة وسهلة الفهم[٣].
- **حق الوصول والتحكم**: ينبغي أن يتمتع الأفراد بحق الوصول إلى بياناتهم الشخصية، وتصحيحها أو طلب حذفها إذا لم تعد هناك حاجة لها[٤].

---

(1) Truong N., Sun K., Lee G. & Guo Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security. Vol 15. https://doi.org/10.1109/TIFS.2019.2948287.

(2) Dreyer J., Heitmann S., Erdmann F., Bauer G. & Kray C. (2022). 'Informed' consent in popular location based services and digital sovereignty. Op. cit. PP 312 – 342.

(٣) اليونسكو. (٢٠٢١). الذكاء الاصطناعي والتعليم: إرشادات لواضعي السياسات. منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو). ص ١٦. والمتاح من خلال الرابط التالي: https://unesdoc.unesco.org/ark:/48223/pf0000380040. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٧.

(4) Dye O., Heo J. & Cankaya E. (2024). Reflection of Federal Data Protection Standards on Cloud Governance. Op. cit.

٢- **حماية البيانات الشخصية**: تتطلب الحماية الفعّالة للبيانات المخزنة على السحابة التزامًا دقيقًا بالإجراءات الأمنية المشددة لضمان الحفاظ على سرية وسلامة هذه البيانات[١]. وهذه بعض الأمثلة للتدابير الأمنية الرئيسية فعلى مزودي الخدمات السحابية تطبيقها:

- **التشفير**: عليهم القيام بالتشفير الكامل والتام للبيانات أثناء النقل وفي أماكن التخزين لضمان عدم وصول الأشخاص غير المصرح لهم إليها[٢].
- **إدارة هويات المستخدمين**: يجب تطبيق نظام إدارة الهويات لضمان أن من يمتلك التصريح وحدهم فقط، من لهم حق التعامل مع البيانات. مع تحديد الصلاحيات[٣].
- **آليات التحكم**: ينبغي تطبيق آليات قوية للتحكم فيمن يمكنه التعامل مع البيانات، بحيث يمنح الوصول إلى البيانات بناءً على الضرورة الوظيفية فقط، مما يضمن حماية أفضل للبيانات الحساسة[٤].

---

(1) Н.Т. Головацький. (2024). Питання захисту персональних даних при використанні хмарних технологій. Аналітично-порівняльне правознавство. № 5. PP 460 – 466. https://doi.org/10.24144/2788-6018.2024.05.72.

(2) Atri P. (2024). Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit. International Journal of Computing and Engineering. Vol 5. Iss4. PP 44 – 55.https://doi.org/10.47941/ijce.1920.

(3) L. Ma, W. Su, B. Wu, B. Yang and X. Jiang. (2022). Joint Emergency Data and Service Evacuation in Cloud Data Centers Against Early Warning Disasters. Op. cit PP 1306 - 1320.

(4) S. Pearson & M. Casassa-Mont. (2011). Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Op. cit. PP 60 - 68.

٣- **إخطار انتهاكات البيانات**: تُعد الإخطار بانتهاكات البيانات من الجوانب الحيوية في "اللائحة العامة لحماية البيانات (GDPR)"، فهي تلزم على مشغلو الخدمات السحابية مسؤولية كبيرة للتصرف بسرعة وشفافية في حالة وقوع اختراق أو انتهاك للبيانات. وهذا الإجراء يهدف إلى تقليل الأضرار المحتملة وحماية حقوق الأفراد المتضررين(١). وهذه الخطوات الأساسية المتبعة عند حدوث انتهاك:

- **تحديد الاختراق**: يجب أن يكون لدى مزودي الخدمات أنظمة لاكتشاف الانتهاكات بسرعة وتحديد نطاقها وأثرها(٢).
- **الإخطار الفوري**: يجب الإبلاغ عن الاختراق إلى الجهات المتخصصة، وأصحاب البيانات خلال ٧٢ ساعة من اكتشافه. يجب أن يتضمن الإخطار تفاصيل عن طبيعة الانتهاك والبيانات المتأثرة والإجراءات المتخذة لمعالجة الوضع(٣).

(1) Zhu J. J., Tuo L., You Y., Fei Q. & Thomson M. (2024). A Preemptive and Curative Solution to Mitigate Data Breaches: Corporate Social Responsibility as a Double Layer of Protection. Journal of Marketing Research. Vol 61. Iss 4. PP 778 - 801. https://doi.org/10.1177/00222437231218969.

(2) Nikkhah H. & Grover V. (2022). An Empirical Investigation of Company Response to Data Breaches. MIS Quarterly. Vol 46. Iss 4. PP 2163 - 2196. https://doi.org/10.25300/misq/2022/16609.

(3) Borgesius F., Asghari H., Bangma N. & Hoepman J. (2023). The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects. SCRIPTed: A Journal of Law, Technology & Society. Vol 20. Iss 2. PP 352 – 381. https://doi.org/10.2218/scrip.20.2.2023.8979.

- **التواصل المستمر**: يجب أن يبقى مزودو الخدمات في تواصل مع السلطات وأصحاب البيانات لتقديم التحديثات والمستجدات حول الإجراءات التصحيحية والتحقيق الجاري[١].

٤- **حق أصحاب البيانات**: حقوق الأفراد في بياناتهم الشخصية وممارستها أمر لا غنى عنه، في "اللائحة العامة لحماية البيانات (GDPR)". هذه الصلاحيات تمنح الأفراد سيطرة أكبر على بياناتهم الشخصية وتساعد في ضمان استخدامها بشكل مسؤول وشفاف[٢]. ومن أهم تلك الحقوق:

- **حق الوصول**: يحق للأفراد طلب الوصول إلى بياناتهم التي يتم تجميعها ومعالجتها، بواسطة مشغلو الخدمات. ويمكنهم طلب نسخة من هذه البيانات لمعرفة كيفية استخدامها[٣].

- **حق النسيان**: يمكن للأفراد طلب حذف أو مسح بياناتهم في الحالات أو الأوقات التي يحددونها، مثل انتهاء الغرض من جمعها أو إذا كانوا يرغبون في سحب موافقتهم على معالجتها[٤].

---

(1) Ibid. PP 352 – 381

(2) Ke T., & Sudhir K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. Management Science. Vol 69. Iss 8. PP 4363-4971. https://doi.org/10.1287/mnsc.2022.4614.

(3) Drechsler L. (2023). Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation. Review of European Administrative Law. https://doi.org/10.7590/187479823x16800083010347.

(4) Susi M. (2020). The Right to Be Forgotten. In A. von Arnauld K. von der Decken & M. Susi (Eds.), The Cambridge Handbook of New Human Rights: Recognition. Novelty. Rhetoric. Chapter. Cambridge: Cambridge University Press. Op. cit. PP 287 – 299.

- **حق التعديل**: يحق للأفراد طلب تصحيح أي معلومات شخصية غير دقيقة أو غير كاملة تخصهم. يجب على مشغلو الخدمات القيام بالإجراء المطلوبة للتعديل، في الوقت المناسب[١].

هذه الحقوق تعزز الثقة بين مزودي الخدمات والمستخدمين، وتضمن عناية أفضل للبيانات.

٥- **نقل المعلومات الرقمية بين البلدان**: تضع اللائحة قيودًا صارمة على نقل البيانات الرقمية الشخصية خارجه، وذلك لضمان أنها تتمتع بنفس مستوى الحماية، حتى عند نقلها إلى دول أخرى. ولتحقيق هذا الهدف، يتعين على مقدمي الخدمات السحابية اتخاذ تدابير قانونية محددة[٢]، مثل:

- **اتفاقيات نقل البيانات**: يجب أن تكون هناك عقود أو اتفاقيات نقل بيانات تضمن أن الجهة المستقبلة للبيانات في الدول الأخرى تلتزم بنفس معايير الحماية[٣].
- **ضمان تكافؤ الحماية**: يجب ضمان توفير الدول المستقبلة للبيانات لمستوى حماية مكافئ للمستوى المطلوب في دول الاتحاد[١].

(1) Dimitra Kamarinou, Christopher Millard & Felicity Turton. (2021). Protection of Personal Data in Clouds and Rights of Individuals', in Christopher Millard (ed.), Cloud Computing Law. 2nd edn Oxford. PP 257 – 293. https://doi.org/10.1093/oso/9780198716662.003.0008.

(2) Christopher Kuner. (2023). Protecting EU data outside EU borders under the GDPR. Common Market Law Review. Vol 60. Iss 1. PP 77 – 106. https://doi.org/10.54648/cola2023004.

(3)Bradford L., Aboy M. & Liddell K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. Journal of Law and the Biosciences. Vol 8. PP 1 – 36. https://doi.org/10.1093/jlb/lsab007.

- **الآليات البديلة**: في حالة عدم توافر اتفاقيات أو عدم امتثال الدول المستقبلة، يجب على مقدمي الخدمات السحابية البحث عن أساليب قانونية بديلة تتضمن حماية تلك البيانات(٢).

من خلال الحفاظ على سرية وسلامة البيانات خلال النقل الدولي، تدعم هذه الإجراءات الثقة في استخدام خدمات الحوسبة السحابية على نطاق عالمي.

إن تحقيق التوازن بين الاستجابة "للائحة العامة لحماية البيانات"، والمرونة يشكل عقبة كبيرة. ففي حين أن العناية بالبيانات وحمايتها أمر ضروري لضمان خصوصيتها، فإن العقبات التي تنظم تلك الخدمات قد تفرض تحديات كبيرة على من يحاول السعي من أفراد أو كيانات للابتكار وتحسين خدماتها(٣).

ولمواجهة هذه التحديات، يمكن للمنظمات اتباع بعض الاستراتيجيات مثل التدريب والتوعية بأهمية الامتثال للائحة، والتعامل مع البيانات بطرق قانونية وآمنة، والاستعانة بخبراء قانونيين متخصصين في المجال لفهم متطلباتهم، والعمل عليها، واستخدام التقنيات المستحدثة، مثل الذكاء الاصطناعي، وذلك لتحسينها وتقليل الأعباء الإدارية، والعمل بشكل وثيق مع الجهات التنظيمية للحصول على توجيهات واضحة وشفافة حول الامتثال. بمساعدة هذه الاستراتيجيات، يمكن للمؤسسات أن تنجح في تحقيق التوازن بين الامتثال التنظيمي والابتكار في خدمات الحوسبة السحابية.

=

(1) Christopher Kuner. (2023). Protecting EU data outside EU borders under the GDPR. Op. cit. PP 77 – 106

(2) Ibi. PP 77 – 106

(3) Maas Matthijs. (2023). Concepts in advanced AI governance A literature review of key terms and definitions. Legal Priorities Project – AI Foundations Report 3. PP 48 – 50. DOI:10.13140/RG.2.2.26115.68647.

٤,٢ القوانين واللوائح المتعلقة بالتخزين السحابي في مصر:

تتجه المؤسسات في مصر نحو الرقمنة، واعتماد الحلول التقنية، وذلك لتعزيز الجدارة، وتحسين الأداء. ويُساهم هذا التوجه في عملية التحول الرقمي، وزيادة الاعتماد على البيانات في اتخاذ القرارات. ومع ذلك، فإن الإطار القانوني المنظم للتخزين السحابي في مصر لا يزال في بدايته، مما يخلق عقبات تتعلق بحفظ البيانات وحمايتها، وخصوصية المستخدمين. وحتى الوقت الحالي لم يصدر المشرع المصري قانونًا خاصًا يتعلق بالتنظيم القانوني للتخزين السحابي، ويرجع ذلك لعدة أسباب منها[١] [٢] [٣]:

١- **نقص الوعي القانوني**: لا يزال هناك نقص في الوعي القانوني بمخاطر وفوائد التخزين السحابي للبيانات في مصر، مما يعقد عملية وضع قوانين منظمة له.

٢- **السرعة والتطور السريع لتقنيات التخزين السحابي**: إذ تتطور تقنياته بسرعة كبيرة، مما يصعب من استحداث أو تعديل قوانين تواكب هذا التطور.

٣- **التعقيد والتعددية**: يعتمد التخزين السحابي في عمله على تقنيات عدة، مما يعقد من وضع قوانين عالمية أو إقليمية.

---

(١) حسام الدين محمود محمد محمد حسن. (٢٠٢٣). واقع الشخصية القانونية للذكاء الاصطناعي. مجلة روح القوانين - كلية الحقوق – جامعة طنطا. عدد ١٠٢. الصفحات ١٠٣ - ٢٤٨. https://doi.org/10.21608/las.2023.189346.1127.

(٢) الموقع الرسمي للمجلس الوطني للذكاء الاصطناعي. https://mcit.gov.eg/ar/Artificial_Intelligence.

(٣) معتز عفيفي. (٢٠٢٣) فلسفة التشريع في مجال الذكاء الاصطناعي. النقابة العامة المصرية للمحامين. والمتاح من خلال الرابط التالي: http://tinyurl.com/yn4qgfo5. وتمت زيارته بتاريخ: ٢٠٢٤/١/١٨.

٤- **عدم اليقين بشأن المخاطر المحتملة**: لا يزال التخزين السحابي مجالًا جديدًا وفي حالة تطور مستمرة، ولذا هناك حالة من عدم اليقين بشأن المخاطر المحتملة المرتبطة باستخدامه.

ومع ذلك، تسعى مصر إلى وضع إطار قانوني عام للتقنيات المستحدثة وتنظيم عملها كالتخزين السحابي، والذكاء الاصطناعي، بحيث يضمن استخدام تلك التقنيات بطريق آمنة ومسؤولة وأخلاقية. وقد كشفت عن خطتها لمواجهة الخطر الداهم الذي سينجم عن التوسع في استخدام تلك التقنيات. حيث أعلن مركز المعلومات ودعم اتخاذ القرار بمجلس الوزراء المصري عن وضع خطة تتضمن خمس مبادئ لمواجهة خطر تلك التقنيات، وهي[١]:

١- تحديد المسؤوليات والمساءلة في استخدام التقنيات.

٢- الحفاظ على خصوصية وسرية البيانات الشخصية.

٣- تحديد أسس وضوابط للاستخدام الأخلاقي والمسؤول للتقنيات الذكية.

٤- تشجيع وتنمية البحث والابتكار في مجال التقنيات الذكية.

٥- زيادة وتفعيل التعاون الدولي في مجال الذكاء الاصطناعي.

---

(١) مستقبل النظام العالمي الجديد. (٢٠٢٣). الإدارة العامة للدراسات المستقبلية والنمذجة، مركز دعم واتخاذ القرار – رئاسة مجلس الوزراء. عدد ٣. والمتاح من خلال الرابط التالي:
https://idsc.gov.eg/upload/DocumentLibraryIssues/AttachmentA/8758/%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84%D9%8A%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B9%D8%AF%D8%AF%20%D8%A7%D9%84%20%D9%A3.pdf.٢٠٢٤/١٢/٢٦ ، وتمت زيارته بتاريخ:

برئاسة وزير الاتصالات وتكنولوجيا المعلومات، تأسس المجلس الوطني للذكاء الاصطناعي في نوفمبر ٢٠١٩، وهو عبارة عن شراكة بين المؤسسات الحكومية، والأكاديميين، والكيانات العاملة في المجال، ويتولى مسؤولية[١] [٢]:

١- إعداد الاستراتيجية الوطنية للذكاء الاصطناعي.

٢- إنشاء آليات لمواصلة تنفيذ الاستراتيجية الوطنية للذكاء الاصطناعي، مع ضمان العناية بالبيانات الشخصية، والخصوصية بما يتماشى مع المعايير الدولية.

٣- تعيين الأولويات المعنية بمجال تطبيقات الذكاء الاصطناعي، والعناية بالبيانات الشخصية.

٤- اقتراح سياسات وطنية وتقديم التوصيات الفنية، والقانونية، والاقتصادية، لتطبيقات الذكاء الاصطناعي، وحماية البيانات الشخصية.

٥- تعزيز التعاون في هذا المجال على المستويين الإقليمي والدولي، بما في ذلك تبادل أفضل الممارسات والخبرات.

كما أصدرت في عام ٢٠٢٣ ميثاق الذكاء الاصطناعي، والذي يحدد التوجيهات العامة لاستخدام الذكاء الاصطناعي في مصر، ويتضمن الميثاق خمس مبادئ رئيسية، هي[٣]:

---

(١) الميثاق المصري للذكاء الصناعي المسؤول. المجلس الوطني للذكاء الصناعي. والمتاح من خلال الرابط التالي:

https://aicm.ai.gov.eg//ar/Resources/EgyptianCharterForResponsibleAIArabic-v1.0.pdf. وتمت زيارته بتاريخ:٢٠٢٤/١٢/٢٦ .

(٢) الاستراتيجية الوطنية للذكاء الاصطناعي. المجلس الوطني للذكاء الاصطناعي. متاح من خلال الرابط التالي: https://ai.gov.eg & https://mcit.gov.eg/ar/Artificial_Intelligence/. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

(٣) الميثاق المصري للذكاء الصناعي المسؤول. مرجع سابق.

١- **البشرية كمقصد**: يجب أن يكون الإنسان هو المستفيد الأول من الذكاء الاصطناعي.

٢- **الشفافية وقابلية التفسير**: يجب أن تكون المعلومات المتعلقة بأنظمة الذكاء الاصطناعي متاحة للجمهور وقابلة للتفسير.

٣- **العدالة**: يجب أن تكون أنظمة الذكاء الاصطناعي عادلة وغير متحيزة.

٤- **المسائلة**: مسؤولية الجهات الفاعلة عن أفعالها في تطوير واستخدام أنظمة الذكاء الاصطناعي أمر ضروري.

٥- **الأمن والأمان**: لا بد من ضمان سلامة وأمان أنظمة الذكاء الاصطناعي.

وفي نفس السياق تعمل الحكومة على وضع قوانين قطاعية تنظم استخدام الذكاء الاصطناعي في مجالات متخصصة، مثل الصحية، والتعليم. ومن المأمول أن تصدر الحكومة المصرية قوانين منظمة بصورة أكبر، وذلك في السنوات القادمة.

كما أن هناك بعض القوانين واللوائح العامة في مصر التي قد تشمل بعض الجوانب للتقنيات المستحدثة. من بين هذه القوانين واللوائح:

١- **قانون حماية المعلومات الشخصية**: والمعروف بالقانون "رقم ١٥١ لسنة "٢٠٢٠، والهدف منه هو حماية البيانات والمعلومات الشخصية، وتنظيم جمعها، واستخدامها، ونقلها. والوصول لها.

والذي يفرض التزامات على مقدمي خدمات التخزين السحابي، يجب الحصول على موافقة واضحة ومباشرة من الأفراد قبل البدء في جمع بياناتهم. كما يحدد متطلبات أمان صارمة لحماية البيانات المخزنة من الوصول غير الأمن. ويمنح الأفراد حقوقًا

مثل الاطلاع على بياناتهم، أو تعديها، أو حتى حذفها، مما يشابه "اللائحة العامة لحماية البيانات (GDPR)".

٢- **قانون الاتصالات وتكنولوجيا المعلومات**: والمعروف بقانون تنظيم الاتصالات "رقم ١٠ لسنة ٢٠٠٣"، والذي ينظم استخدام التكنولوجيا والاتصالات. ويتضمن مجموعة من القواعد التي تهدف إلى الحفاظ على الأمن السيبراني، وحماية البيانات، كما هناك بعض من القرارات الصادرة من بعض الوزارات، واللوائح التي تشرح بنود هذا القانون.

٣- **قانون مكافحة جرائم تقنية المعلومات**: والمعروف بقانون "رقم ١٧٥ لسنة ٢٠١٨"، حيث يعتبر هذا القانون الذي اساس للتشريعات الخاصة بالجرائم الإلكترونية؛ فهو يحدد العقوبات المفروضة على اختراق البيانات الالكترونية، وعلى الوصول غير المصرح به، وانتهاكات خصوصية البيانات، وغيرها من أشكال المخالفات الالكترونية.

كما يحدد عقوبات صارمة للاختراق غير المشروع أو تسريب البيانات المخزنة عبر الخدمات السحابية. كما يلزم مقدمي الخدمات بالتعاون مع الجهات الأمنية للكشف عن الجرائم المتعلقة بالبيانات المحفوظة بشكل إلكتروني.

وبالتالي؛ تسعى الحكومة في مصر إلى وضع نظم قانونية تضمن حماية البيانات وسلامتها، مع توفير بيئة تحمي حقوق الأفراد وتدعم الابتكار في استخدام خدمات التخزين السحابي. ولضمان الاستفادة الآمنة والمستدامة من التخزين السحابي، يجب على مصر اتباع أفضل الممارسات، مع تبني المعايير الدولية.

٤,٣ القوانين واللوائح المتعلقة بالتخزين في الكويت:

تبنت الكويت نظامًا قائمًا على التقنيات الرقمية، وذلك خلال الأعوام القليلة الماضية، وأدى ذلك إلى زيادة اعتماد الأفراد والمؤسسات على حلول التخزين السحابي. يُعد التخزين السحابي جزءًا أساسيًا من هذا السياق القائم على التحول الرقمي، إذ يوفر إمكانية تخزين البيانات والوصول إليها بشكل مرن وآمن. ومع تزايد أهميته، برزت الحاجة تنظيم استخدام هذه التقنيات المستحدثة، لضمان حماية البيانات وتعزيز الثقة في بيئة السحابة.

لم ينص الدستور الكويتي على الحق في حماية الخصوصية، أو البيانات الشخصية الإلكترونية بشكل مباشر بطبيعة الأمر. ولكن يُستند في هذا إلى المبادئ الدستورية مثل حماية الحرية الشخصية والكرامة الإنسانية، والتي تنص عليها المادة ٣٠ من الدستور. وقد دعمت المحكمة الدستورية الكويتية هذا الاجراء من خلال الحكم رقم ٣ لسنة ١٩٨٢، مؤكدةً على أهمية صون الكرامة وعدم انتهاك الأسرار الشخصية[١].

(١) يعتبر حكم المحكمة الدستورية الكويتية رقم ٣ لسنة ١٩٨٢ من الأحكام البارزة في تاريخ القضاء الكويتي، حيث تناول قضية مهمة تتعلق بحدود الحقوق والحريات في المجتمع. هذا الحكم ألقى الضوء على التوازن الدقيق بين حق الشكوى كحق دستوري وواجب احترام النظام العام والأخلاق العامة.

تناول الحكم قضية تتعلق بحق الشكوى الذي يضمنه الدستور، ومدى حدود هذا الحق. أكدت المحكمة أن حق الشكوى ليس حقًا مطلقًا، بل يخضع لضوابط وقواعد تحكم ممارسته. وأشارت إلى أن هذا الحق يجب أن يمارس ضمن إطار احترام النظام العام والأخلاق العامة، وعدم التعدي على حقوق الآخرين.

محمد عبدالقادر الجاسم. (٢٠٠٩). دار قرطاس للنشر.

وبالرغم من أن الدستور الكويتي لا ينص بشكل صريح على حماية البيانات، إلا أن المبادئ القانونية، والدستورية توفر الأسس القانونية المطلوبة للحماية. والتي تُعتبر جزءًا من الحق الذي ينظمه الدستور في صون الحياة الخاصة، وبهذا لا يمكن التعامل مع البيانات المحفوظة، أو كشفها إلا بموافقة المعني بها.

ورغم وجود هذه القوانين، إلا أن عقبات كثيرة، للتعامل مع الاحداث السريعة للتخزين السحابي. يتطلب الوضع الحالي وضع سياق قانوني أكثر استيعاب، يتماشى مع القواعد الدولية، مثل "اللائحة العامة لحماية البيانات (GDPR)"، لمواكبة التصاعد المتزايد للتقنيات السحابية، وتلبية رغبة العملاء.

وعلى المستوى التشريعي، ترتكز الحماية للبيانات الشخصية، والتخزين السحابي إلى عدد من القوانين، والتي تضع الطرق القانونية المزمع اتباعها من قبل الشركات والمؤسسات الحكومية والخاصة. وفيما يلي أبرز تلك القوانين:

١- **القانون "رقم ٢٠ لسنة ٢٠١٤" الخاص بالمعاملات الإلكترونية**: ويهدف إلى تنظيم المعاملات الإلكترونية، مع وضع أسس قانونية معنية بحماية البيانات وخاصة الشخصية منها. يحتوي الشق السابع من القانون على أحكام محددة تتعلق بالخصوصية، حيث يلزم الحكومة، والكيانات الخاصة بالحفاظ على سرية المعلومات، وخاصة الشخصية منها، وعدم الإفصاح عنها إلا بموافقة صريحة من الشخص المعني أو بتفويض قانوني. كما يمنح الأفراد حقوقًا واضحة في التعامل مع بياناتهم المخزنة لدى المؤسسات المختلفة، ما يعزز من حماية خصوصيتهم[١].

(١) قانون رقم ٢٠ لسنة ٢٠١٤. (٢٠١٤). قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية. مجلس الوزراء – الجهاز المركزي لتكنولوجيا المعلومات. مرجع سابق.

٢- **القانون "رقم ٣٧ لسنة ٢٠١٤" "الخاص بإنشاء الهيئة العامة للاتصالات وتقنية المعلومات (CITRA)":** والذي أنشأ الهيئة العامة للاتصالات كجهة تنظيمية مسؤولة عن قطاع الاتصالات والمعلومات في دولة الكويت، فالمادة رقم ٣ منه، تفويض الهيئة بوضع لوائح من شأنها أن تعمل على حماية البيانات وخاصة الشخصية منها. وتماشيًا مع هذا الدور، أصدرت الهيئة لائحة رقم ٢١ لعام ٢٠٢١ بشأن حماية خصوصية البيانات، التي تحدد القواعد والإرشادات الخاصة بحماية البيانات الشخصية في قطاع الاتصالات(١).

٣- **اللائحة "رقم ٢١ لسنة ٢١" المعنية بحماية البيانات**: تُعد تلك والصادرة عن "الهيئة العامة للاتصالات وتقنية المعلومات" بموجب قانون الاتصالات، إطارًا تنظيميًا مهمًا يهدف إلى حماية البيانات وخاصة الشخصية منها. عرّفت اللائحة (البيانات الشخصية "بأنها أي معلومات تتعلق بشخص طبيعي أو اعتباري يمكن تحديد هويته من خلالها بشكل مباشر، مثل الاسم والهوية والمعلومات المالية والصحية، والبيانات الجغرافية، والبصمات الوراثية، والصوتية").

وتُطبق أحكام اللائحة على الأشخاص الطبيعيين والاعتباريين الذين يقومون بجمع أو معالجة البيانات الشخصية باستخدام مراكز معلومات لتقديم خدمات تقنية المعلومات، سواء في القطاع العام أو الخاص، مع استثناء الأنشطة الشخصية أو العائلية والجهات الأمنية التي تجمع لأغراض الأمن العام.

---

(١) قانون إنشاء الهيئة العامة للاتصالات وتقنية المعلومات. (ب. ت.). الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي: https://citra.gov.kw/sites/ar/Pages/CITRAEstablishmentLaw.aspx. وتمت زيارته بتاريخ:٢٠٢٤/١٢/٢٧.

كما حددت اللائحة مفهوم "المعالجة الإلكترونية" بأنها أي عملية تقوم على البيانات الشخصية باستخدام وسائل الكترونية، أو غير الكترونية، بما في ذلك التعامل بكافة الصور كجمعها، أو تخزينها أو الاتلاف. ونطاق التطبيق الواسع لهذه اللائحة يعطي نهجًا شاملًا يعمل على تعزيز الحماية الفائقة البيانات، وتنظيم أسواق الخدمات السحابية، وضمان توافق القوانين داخل الدولة مع القوانين الدولية مثل "اللائحة العامة لحماية البيانات (GDPR)". ومع ذلك، يتطلب هذا الإطار القانوني تحديثًا مستمرًا لمواكبة التطورات التقنية وضمان الالتزام الفعّال بلوائح حماية البيانات.

وهذه اللائحة تخضع للتحديث المستمر، وتحظى باهتمام كبير من قبل المنظمين الكويتيين، وقد جري عليها مجموعة من التحديثات أخرها الإصدار ٢,٥ الذي تم صدوره بتاريخ ٢٠٢٤/٢/١٨[١].

٤- **قوانين أخرى ذات صلة بالتخزين السحابي في الكويت**: إلى جانب لائحة حماية الخصوصية، هناك قوانين أخرى تُسهم في تنظيم التخزين السحابي واستخدام البيانات، أبرزها:

- **قانون التجارة الإلكترونية**: يُعد هذا القانون الأساسي الذي ينسق المعاملات الالكترونية، واستخدام التقنيات المستحدثة في العمليات التجارية الالكترونية. ويشمل ذلك تنسيق عمليات التعاقد الرقمي وتخزين البيانات السحابية المستخدمة

(١) لائحة حماية البيانات والخصوصية الإصدار ٢,٥. (٢٠٢٤). الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي: https://tinyurl.com/25pft52r. وتمت زيارته بتاريخ:٢٠٢٤/١٢/٢٧.

في التجارة الإلكترونية، مما يضمن حماية البيانات وضمان استمرارية الأعمال الرقمية بشكل آمن وقانوني.

- **القوانين الاخرى:** تخضع بعض القطاعات ذات الحساسية العالية، مثل القطاع المصرفي والقطاع الصحي، لمتطلبات تنظيمية خاصة تحكم كيفية جمع ومعالجة وتخزين البيانات. على سبيل المثال، تفرض هذه القوانين معايير أمان مشددة عند استخدام التخزين السحابي، بما يتوافق مع أعلى معايير السرية والخصوصية.

تشكل هذه القوانين مجتمعة إطارًا شاملًا يضمن تنظيم استخدام التخزين السحابي في مختلف القطاعات، مع منح الحماية اللازمة للبيانات في دولة الكويت.

من خلال القوانين الحالية والتطورات التشريعية المرتقبة، تطمح الدولة إلى بناء بيئة قانونية، لدعم استخدام خدمات التخزين السحابي بما يتماشى مع التحول الرقمي المتسارع. وتهدف هذه الجهود إلى تحقيق توازن بين تشجيع اعتماد التقنيات المستحدثة في تخزين المعلومات وإدارتها، مع رعاية حق الأفراد وحماية خصوصيتهم. كما تولي التشريعات اهتمامًا خاصًا لضمان أمن البيانات، ومسايرة التطورات العالمية. والجدول التالي يوضح مقارنة بين الأطر في كلًا من القانون الأوروبي والكويتي والمصري.

جدول رقم (١)

مقارنة بين الأطر في كلًا من القانون الأوروبي والكويتي والمصري

العنصر	الاتحاد الأوروبي (GDPR)	الكويت	مصر
شمولية التشريع	متقدم وشامل	محدود	متوسط
حقوق أصحاب البيانات	واضحة وصارمة	محدودة	قيد التطوير
السيادة على البيانات	توازن بين نقل البيانات والسيادة الوطنية	ضعف التنسيق الدولي	التركز على البيانات المحلية
الامتثال الدولي	يفرض متطلبات على مقدمي الخدمات العالميين	محدود	محدود
العقوبات	كبيرة ورادعة	متوسطة	محدودة

الجدول من اعداد الباحث

تحديات التنظيم القانوني للتخزين السحابي:

يواجه التنظيم القانوني للتخزين السحابي على الصعيد العالمي بصفة عامة، والصعيد المحلي بصفة خاصة العديد من التحديات، خاصة مع التباين في الأطر التشريعية بين الدول. وفيما يلي أبرز العقبات والفروقات:

١- **نفوذ الشركات على أصحاب القرار**: سنة ٢٠٢١، تبين للمفوضية الأوروبية أن الحوسبة السحابية تشكل ثغرة رئيسية تستدعي تعزيزًا تنظيميًا وتقنيًا لضمان الامتثال

ورعاية البيانات وحمايتها[١]. وجاءت استجابتها بالموافقة على مدونتين لقواعد السلوك تم تطويرهما بواسطة قادة الصناعة بالتعاون مع الشركات العاملة في هذا المجال[٢].

وهذا التدخل يظهر القوة والنفوذ الذي تمتلكه الشركات على صانعي القرار، حيث تعتمد الجهات التنظيمية على الخبرات والمعرفة الفنية للشركات لتطوير حلول تتماشى مع النظم الحالية. وتحسين الثقة في سوق الحوسبة داخل دول الاتحاد الأوروبي[٣].

ونفوذ الشركات يتضح بصورة أكبر في وضع القواعد الخاصة بالتخزين السحابي من خلال الاستفادة من خبراتها الفنية والقانونية، وهو ما لا يمتلكه بالضرورة مستخدم الخدمة[٤]. وهذا الفارق في المعرفة يمكن أن يؤدي إلى وضع شروط

(1) Bania K., & Geradin D. (2023). The regulation of cloud computing: why the European Union failed to get it right. Information & Communications Technology Law. Vol 33. Iss 1. PP 99 - 113. https://doi.org/10.1080/13600834.2023.2260687.

(2) Blancato, F. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet. Vol 16. PP 12 – 32. https://doi.org/10.1002/poi3.358.

(3) Li Y., Shi H. & Zhou Y. (2021). The influence of the media on government decisions: Evidence from IPOs in China. Journal of Corporate Finance. Vol 70. PP 102056. https://doi.org/10.1016/J.JCORPFIN.2021.102056.

(٤) نقص الوعي القانوني والتقني يُعتبر من التحديات البارزة التي تواجه كل من المستخدمين والمؤسسات عند التعامل مع التخزين السحابي.

١- **عند المستخدمين**: غالبًا ما يكون هناك عدم فهم كامل للشروط القانونية والحقوق المتعلقة بالبيانات المخزنة. وهذا يمكن أن يؤدي إلى قلة الوعي بمخاطر الأمان والخصوصية والاعتماد على مقدمي الخدمات بشكل مفرط دون اتخاذ الاحتياطات اللازمة.

٢- **عند المؤسسات**: قد تعاني بعض المؤسسات من ضعف المعرفة بالتزاماتها القانونية عند استخدام التخزين السحابي. وهذا يشمل الامتثال للتشريعات المحلية والدولية بشأن حماية البيانات، وضمان تطبيق تدابير الأمان المناسبة لحماية بيانات العملاء.

وقواعد قد تكون أكثر تفضيلًا للشركات، مما يسهل عليها التنصل من المسؤولية عن الأضرار الناتجة عن تسرب أو فقد البيانات الخاصة بالمستخدمين.

فوجود هذا النفوذ يبرز أهمية التوعية وتوضيح المسؤولية في قطاع الحوسبة السحابية، يضمان حماية حقوق المستخدمين وتحقيق توازن عادل بين مقدمي الخدمات والمستخدمين(١).

٢- **التباين التشريعي بين الدول**: التباين التشريعي بين الدول من أكبر العقبات التي تقابل الحوسبة السحابية، وحماية البيانات. فعلى مستوى الدول تختلف الانظمة القانونية المعنية بالبيانات والتنظيم السحابي بشكل كبير بين الدول، مما يؤدي إلى صعوبات في الامتثال القانوني عند تقديم خدمات عالمية. هذه الاختلافات قد تتضمن معايير الحماية، ومتطلبات الأمان، وحقوق التعامل مع البيانات(٢).

فمثلًا، في بعض الدول مثل الكويت ومصر، قد يكون هناك غياب لأطر قانونية متكاملة تغطي جميع جوانب التخزين السحابي. وهذا القصور يصعب على مقدمي الخدمات الالتزام بمعايير موحدة وحماية بيانات المستخدمين بشكل فعال. وفي المقابل، تتبنى دول أخرى كالاتحاد الأوروبي قوانين شاملة مثل "اللائحة العامة لحماية البيانات (GDPR)"، التي تحتوي على معايير صارمة معنية بحماية البيانات.

(1) Dye O., Heo J. & Cankaya E. (2024). Reflection of Federal Data Protection Standards on Cloud Governance. Op. cit.

(2) Hazrat Usman, Iqra Tariq & Bushra Nawaz. (2023). IN THE REALM OF THE MACHINES: AI'S INFLUENCE UPON INTERNATIONAL LAW AND POLICY. JOURNAL OF SOCIAL RESEARCH DEVELOPMENT. Vol 4. Is 2. PP 383 – 399. https://doi.org/10.53664/JSRD/04-02-2023-13-383-399.

وهذا التباين يتطلب من القائمين على التخزين السحابي أن تكون لديهم المرونة والقادرة على التكيف مع تلك اللائحة. ويبرز أهمية التعاون الدولي لتطوير أطر قانونية موحدة تعزز حماية البيانات على مستوى عالمي[١].

٣- **السيادة على البيانات**: السيادة على البيانات تعد أحد القضايا الرئيسية التي تثير العديد من العقبات القانونية، خاصة عند تخزين البيانات خارج الحدود الوطنية. وتخزين البيانات في مراكز بيانات تقع في دول أخرى قد يثير تساؤلات حول سيطرة الدول على تلك البيانات وحقوق الوصول إليها وحمايتها. وهذا من شأنه أن يؤدي إلى مخاوف بشأن انتهاك خصوصيتها، وضمان التعامل معها وفقًا للقوانين[٢].

مثال على ذلك، يمكن أن تؤدي القوانين المتضاربة إلى تعقيدات قانونية كبيرة. فقانون الوصول إلى البيانات الخاص بالولايات المتحدة الأمريكية (Cloud Act) يمنح الحق للسلطات فيها طلب الوصول إلى البيانات المحفوظة في المؤسسات الموجودة خارج الدولة، وهذا قد يتعارض مع قوانين الدول الأخرى، إذ قد تفرض قيودًا صارمة على البيانات وخاصة الشخصية منها، أو الوطنية[٣].

(1) Hazrat Usman, Iqra Tariq & Bushra Nawaz. (2023). IN THE REALM OF THE MACHINES: AI'S INFLUENCE UPON INTERNATIONAL LAW AND POLICY. Op. cit. PP 383 – 399

(2) Меньшиков П.В. & Михина Л. К. (2022). Система противодействия угрозам информационной безопасности КНР// Вестник Забайкальского государственного университета. Op. cit. PP 124 - 139.

(3) Blessing G., Azeta A., Misra S., Osamor V., Sanz L., & Pospelova V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial IntelligenceVol 36. Is 1. https://doi.org/10.1080/08839514.2022.2037254.

وهذا التباين القانوني يتطلب وضع إجراءات صريحة لضمان الالتزام بالقوانين المختلفة، بالإضافة إلى تعزيز التعاون الدولي لوضع نظم قانونية موحدة تعزز حماية البيانات على مستوى عالمي.

٤- **دور مقدمي الخدمات السحابية في تحمل المسؤولية**: المسؤولية من أهم الاساسيات التي يجب تحديدها بوضوح، من أجل حماية البيانات. إذ ينبغي على مقدمي الخدمات السحابية تحديد مسؤولية كل طرف، بشكل واضح، خاصة عند حدوث تسريب لها أو فشل الخدمة. كما أن توزيع المسؤولية بين الأطراف يعد أمرًا بالغ الأهمية، خاصة الأنواع المتشاركة، إذ يكون هناك تعاون بين مقدمو الخدمة والمستخدمين لتقديم الخدمات السحابية[١].

من ناحية أخرى، يظل غياب التوحيد القياسي تحديًا كبيرًا، وافتقار المعايير الدولية يؤدي إلى تفاوت في جودة الخدمة والأمان بين المزودين، مما يؤثر على الثقة في الخدمات السحابية[٢].

(1) Islam M. (2024). Protecting Data Access Liabilities in Cloud Computing. Journal of Artificial Intelligence General science (JAIGS). Vol 3. Iss1. PP 180 – 200. ISSN:3006-4023. https://doi.org/10.60087/jaigs.vol03.issue01.p195.

(2) Ranjan, R. (2014). The Cloud Interoperability Challenge. IEEE Cloud Computing. Vol 1. Iss 2. PP 20 - 24. https://doi.org/10.1109/MCC.2014.41.

الخاتمة:

يمثل التخزين السحابي ركيزة أساسية للتحول الرقمي، حيث توفر إمكانات هائلة لتحسين كفاءة تخزين البيانات ومعالجتها. ومع ذلك، فإن التقدم المتسارع يفرض عقبات قانونية متنوعة، وخاصة التي تتعلق بحماية وحفظ البيانات وحقوق الأفراد. تناولت هذه الدراسة التنظيم القانوني للتخزين السحابي من خلال مقارنة بين الإطار القانوني الأوروبي، الذي يُعتبر نموذجًا عالميًا في سياق حماية وحفظ البيانات، تشهد دول أخرى كمصر والكويت تقدمًا تدريجيًا في تنظيم هذا القطاع الحيوي.

وأظهرت الدراسة أن الاتحاد الأوروبي يقدم إطارًا شاملًا من خلال اللائحة العامة لحماية البيانات (GDPR)، والتي تهدف إلى توحيد مقاييس حماية وحفظ البيانات بين الدول داخل الاتحاد، وتحسين الشفافية والثقة بين المستخدمين ومقدمي الخدمات السحابية. يوفر هذا الإطار تنظيمًا دقيقًا للتعامل مع البيانات، مع الثبات على حقوق الأفراد في الحصول والتعامل مع البيانات الخاصة بهم. كما تفرض اللائحة التزامات مشددة على الشركات للالتزام بها، مما يحسن من مستوى الأمن.

أما في الكويت، فقد تبين أن القوانين مثل "قانون المعاملات الإلكترونية" و"لائحة حماية الخصوصية" الصادرة عن الهيئة العامة للاتصالات وتقنية المعلومات تقدم نموذجا قانونيًا ناشئًا يهدف إلى تنظيم استخدام البيانات الشخصية والتعامل معها في السياق السحابي. ومع ذلك، تحتاج هذه القوانين إلى مزيد من التحديث والشمولية لمسايرة التقنيات العالمية، ولتغطية جوانب أكثر تفصيلًا تتعلق بمعالجة البيانات عبر الحدود والأمن السيبراني.

وفي مصر، يُظهر الإطار القانوني تطورًا تدريجيًا من خلال "قانون حماية البيانات الشخصية" الذي تم إقراره حديثًا. حيث يضع هذا القانون رؤى أساسية معنية

حماية بحفظ البيانات وحمايتها، إلا أن الواقع الفعلي يتطلب مزيدًا من التوجيهات واللوائح التنفيذية لضمان كفاءة التنفيذ ومواكبة الممارسات الدولية.

وخلصت الدراسة إلى أن هناك تباينًا ملحوظًا في تطور الأطر القانونية بين الدول محل الدراسة، حيث تتفوق أوروبا بإطار قانوني ناضج ومتكامل، بينما لا تزال الكويت ومصر في مراحل تطويرية تحتاج إلى بزل المزيد من الجهود، والتضافر بين الشركاء المعنين للتعامل مع العقبات المتعلقة بالتخزين السحابي.

التوصيات:

بناءً على ما تم تناوله في الدراسة، ومن خلال المقارنة بين التنظيم القانوني للتخزين السحابي في الاتحاد الأوروبي والكويت ومصر، توصي الدراسة بالتوصيات التالية:

أولًا: على المستوى الدولي:

١- **تحديث التشريعات بشكل مستمر**: ضرورة مواكبة التشريعات للتقدم في التقنيات المعنية بالتخزين السحابي، مع التركيز على مرونة في التشريعات المقترحة، وقابليتها للتكيف.

٢- **التعاون الدولي**: الحرص على التعاون الفعال بين الدول، وذلك لتبادل الخبرات، واقتراح الحلول الخاص بتنظيم التخزين السحابي، ووضع معايير مشتركة بين الدول.

٣- **تطوير القيادة المؤهلة**: الاستثمار في تطوير الكوادر المؤهلة في مجال الأمن السيبراني والقانون الرقمي، لتلبية احتياجات السوق المتزايدة.

٤- **مراعاة الخصوصيات المحلية:** تصميم التشريعات بما يتماشى مع البيئات الاجتماعية والثقافية والاقتصادية لكل دولة. مع ضمان أن يكون هناك توازن بين حماية الحقوق، وتشجيع الاستثمار في تقنيات الحوسبة السحابية.

٥- **التوعية**: رفع مستوى المعرفة لدى الأفراد والكيانات بأهمية حماية البيانات وكيفية استخدام خدمات التخزين السحابي بشكل آمن.

٦- **إنشاء هيئة مستقلة لحماية البيانات**: إنشاء هيئة مستقلة لحماية البيانات في كل دولة، تكون مسؤولة عن تطبيق التشريعات المتعلقة بحماية وحفظ البيانات، والتحقيق من الانتهاكات.

٧- **تطوير آليات تسوية المنازعات**: تطوير آليات فعالة لتسوية المنازعات التي قد تنشأ بين مزودي الخدمات والمستخدمين.

٨- **تشجيع التعاون الشركاء**: تشجيع التعاون بين الحكومات والأفراد والكيانات، وذلك لتقديم حلول مبتكرة لتجاوز العقبات في التخزين السحابي.

ثانيًا: على مستوى الدول محل الدراسة:

١- الاتحاد الأوروبي:

- **تقييم تطبيق الـ GDPR**: تقييم مدى فعالية تطبيق "اللائحة العامة لحماية البيانات (GDPR)" في مجال التخزين السحابي، وإجراء التعديلات اللازمة لزيادة فعاليتها.
- **تشجيع التعاون مع الدول خارج الاتحاد**: تشجيع التعاون مع الدول خارج الاتحاد لوضع معايير دولية لحماية وحفظ البيانات.

٢- مصر:

- **وضع تشريع شامل**: وضع تشريع شامل ومتكامل ينظم جميع جوانب التخزين السحابي، مع التركيز على لحماية وحفظ البيانات وخاصة الشخصية، وضمان وحقوق الأفراد.
- **تعديل قانون حماية وحفظ البيانات الشخصية**: تعديل القوانين السارية لتحتوي بشكل أكثر تفصيلًا أحكامًا تتعلق بالتخزين السحابي، وتكييفه مع المعايير الدولية.
- **تحسين دور الجهاز القومي لتنظيم الاتصالات**: وذلك بتكليفه بدور أكبر في تنظيم قطاع التخزين السحابي، وتزويده بالصلاحيات اللازمة.

٣- الكويت:

- **مراجعة الوضع التنظيمي**: مراجعة الوضع الحالي بشكل دوري، من أجل مسايرة التطورات التقنية، وتحديث القوانين الوطنية.
- **توسيع نطاق الرقابة**: توسيع نطاق الرقابة على مزودي خدمات التخزين السحابي لضمان التزامهم بالمعايير المحددة.
- **تشجيع الابتكار**: وضع سياسات تشجع على الابتكار في مجال التخزين السحابي، مع الحفاظ على مستوى عالٍ من حماية البيانات.

وهذه التوصيات تهدف إلى سد الثغرات القانونية الحالية، وتساعد في قيام التوازن بين الابتكار، وحفظ وصون الحقوق من خلال بناء نظام قانوني متكامل ومتطور، لضمان بيئة آمنة لاستخدام التخزين السحابي.

قائمة المراجع

أولًا المراجع العربية:

الاستراتيجية الوطنية للذكاء الاصطناعي. المجلس الوطني للذكاء الاصطناعي. متاح من خلال الرابط التالي:

https://mcit.gov.eg/ar/Artificial_Intelligence & https://ai.gov.eg/ . وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

حسام الدين محمود محمد محمد حسن. (٢٠٢٣). واقع الشخصية القانونية للذكاء الاصطناعي. مجلة روح القوانين - كلية الحقوق – جامعة طنطا. عدد ١٠٢. الصفحات ١٠٣ - ٢٤٨. https://doi.org/10.21608/las.2023.189346.1127.

سياسة الخصوصية. (ب. ت.). رؤية السعودية ٢٠٣٠. ومتاح من خلال الرابط التالي: https://www.vision2030.gov.sa/ar/annual-reports . وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

القانون الاتحادي لحماية البيانات الشخصية. (٢٠٢٤). قوانين حماية البيانات. البوابة الرسمية لحكومة دولة الإمارات العربية المتحدة. ومتاح من خلال الرابط التالي:

https://u.ae/ar-ae/about-the-uae/digital-uae/data/data-protection-laws . وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

قانون إنشاء الهيئة العامة للاتصالات وتقنية المعلومات. (ب. ت.). الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي:

https://citra.gov.kw/sites/ar/Pages/CITRAEstablishmentLaw.aspx . وتمت زيارته بتاريخ:٢٠٢٤/١٢/٢٧.

قانون رقم ٢٠ لسنة ٢٠١٤. (٢٠١٤). قانون رقم ٢٠ لسنة ٢٠١٤ في شأن المعاملات الإلكترونية. مجلس الوزراء – الجهاز المركزي لتكنولوجيا المعلومات. ومتاح من خلال الرابط التالي:

https://www.e.gov.kw/sites/kgoArabic/Forms/MagazineA.pdf . وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

لائحة حماية البيانات والخصوصية الإصدار ٢,٥. (٢٠٢٤). الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي: https://tinyurl.com/25pft52r. وتمت زيارته بتاريخ:٢٠٢٤/١٢/٢٧.

محمد عبدالقادر الجاسم. (٢٠٠٩). دار قرطاس للنشر.

مستقبل النظام العالمي الجديد. (٢٠٢٣). الإدارة العامة للدراسات المستقبلية والنمذجة، مركز دعم واتخاذ القرار – رئاسة مجلس الوزراء. عدد ٣. والمتاح من خلال الرابط التالي:

https://idsc.gov.eg/upload/DocumentLibraryIssues/AttachmentA/8758/%D9%85%D8%B3%D8%AA%D9%82%D8%A8%D9%84%D9%8A%D8%A7%D8%AA%20%D8%A7%D9%84%D8%B9%D8%AF%D8%AF%20%D8%A7%D9%84%20%D9%A3.pdf ، وتمـــت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

معتز عفيفي. (٢٠٢٣) فلسفة التشريع في مجال الذكاء الاصطناعي. النقابة العامة المصرية للمحامين. والمتاح من خلال الرابط التالي:

. وتمت زيارته بتاريخ: ٢٠٢٤/١/١٨. http://tinyurl.com/yn4qgfo5

الموقع الرسمي للمجلس الوطني للذكاء الاصطناعي.

https://mcit.gov.eg/ar/Artificial_Intelligence .

الميثاق المصري للذكاء الصناعي المسؤول. المجلس الوطني للذكاء الصناعي. والمتاح من خلال الرابط التالي:

https://aicm.ai.gov.eg//ar/Resources/EgyptianCharterForResponsibleAIArabic-v1.0.pdf.٢٠٢٤/١٢/٢٦ . وتمت زيارته بتاريخ:

الهيئة العامة للاتصالات وتقنية المعلومات. ومتاح من خلال الرابط التالي: https://citra.gov.kw/sites/Ar/Pages/AboutUs.aspx. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٦.

اليونسكو. (٢٠٢١). الذكاء الاصطناعي والتعليم: إرشادات لواضعي السياسات. منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو). ص ١٦. والمتاح من خلال الرابط التالي: https://unesdoc.unesco.org/ark:/48223/pf0000380040. وتمت زيارته بتاريخ: ٢٠٢٤/١٢/٢٧.

ثانيًا المراجع الأجنبية:

A. M. Shuvo, M. S. Amin & P. Haque. (2020). Storage Efficient Data Security Model for Distributed Cloud Storage. 2020 IEEE 8th

R10 Humanitarian Technology Conference (R10-HTC). Kuching, Malaysia. PP 1 - 6. doi: 10.1109/R10-HTC49770.2020.9356962.

Abadi A. (2022). Smarter Data Availability Checks in the Cloud: Proof of Storage via Blockchain. In M. Wynn (Ed.), Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies. IGI Global Scientific Publishing. PP 320 - 339. https://doi.org/10.4018/978-1-7998-7712-7.ch017

Abuhamra E., Ali E., & Ali E. (2024). Improving Cloud Database Performance Using Storage Technologies. IOSR Journal of Computer Engineering. Vol 26. Iss 5. PP 61 – 65. https://doi.org/10.9790/0661-2605036165.

Adhab A. H., & Hussien N. A. (2023). Study of Efficient Cloud Storage Architectures for the Security Environment. Journal of Kufa for Mathematics and Computer. Vol 10. Iss 1. PP 63 – 71. https://doi.org/10.31642/JoKMC/2018/100108.

Andriole, K. (2014). Security of electronic medical information and patient privacy: what you need to know. Journal of the American College of Radiology (JACR). Vol 11. Iss 12. PP 1212 - 1216. https://doi.org/10.1016/j.jacr.2014.09.011.

Atri P. (2024). Enhancing Big Data Security through Comprehensive Data Protection Measures: A Focus on Securing Data at Rest and In-Transit. International Journal of Computing and Engineering. Vol 5. Iss4. PP 44 – 55.https://doi.org/10.47941/ijce.1920.

Awasthi M. (2022). Verifiable and Practical Compliance for Data Privacy Laws. 2022 IEEE 29th International Conference on High Performance Computing, Data and Analytics Workshop (HiPCW). PP 59-60. https://doi.org/10.1109/HiPCW57629.2022.00013.

B. Li, Q. He, F. Chen, H. Jin, Y. Xiang and Y. Yang. (2021). Auditing Cache Data Integrity in the Edge Computing Environment. in IEEE Transactions on Parallel and Distributed Systems. Vol 32. Iss 5. PP 1210 – 1223. doi: 10.1109/TPDS.2020.3043755.

Babu M.R., Nikhitha T., Naheeda S., Kethan S., Sainath P. & Jaswanth, V. (2023). A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage. In: Choudrie J., Mahalle P.N. Perumal T., Joshi A. (eds) IOT with Smart Systems. ICTIS 2023. Lecture Notes in Networks and Systems. Springer, Singapore. Vol 720. PP 217–228. https://doi.org/10.1007/978-981-99-3761-5_21.

Bakare S., Adeniyi A., Akpuokwe C. & Eneh N. (2024). DATA PRIVACY LAWS AND COMPLIANCE: A COMPARATIVE REVIEW OF THE EU GDPR AND USA REGULATIONS. Computer Science & IT Research Journal. Vol 5. Iss 3. PP 528 - 543. https://doi.org/10.51594/csitrj.v5i3.859.

Bania K., & Geradin D. (2023). The regulation of cloud computing: why the European Union failed to get it right. Information & Communications Technology Law. Vol 33. Iss 1. PP 99 - 113. https://doi.org/10.1080/13600834.2023.2260687.

Blancato, F. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. Policy & Internet. Vol 16. PP 12 – 32. https://doi.org/10.1002/poi3.358.

Blessing G., Azeta A., Misra S., Osamor V., Sanz L., & Pospelova V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial IntelligenceVol 36. Is 1. https://doi.org/10.1080/08839514.2022.2037254.

Borgesius F., Asghari H., Bangma N. & Hoepman J. (2023). The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects. SCRIPTed: A Journal of Law, Technology & Society. Vol

20. Iss 2. PP 352 – 381. https://doi.org/10.2218/scrip.20.2.2023.8979.

Bradford L., Aboy M. & Liddell K. (2021). Standard contractual clauses for cross-border transfers of health data after Schrems II. Journal of Law and the Biosciences. Vol 8. PP 1 – 36. https://doi.org/10.1093/jlb/lsab007.

California Consumer Privacy Act (CCPA). (2024). State of California Department of Justice. Available through the following link https://oag.ca.gov/privacy/ccpa. It was viewed on: 25/12/2024.

Celesti A., Fazio M., Villari M. & Puliafito A. (2016). Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems. Journal of Network and Computer Applications. Vol 59. PP 208 - 218. https://doi.org/10.1016/j.jnca.2014.09.021.

Chaudhuri R. & Joseph, A. (2024). Living in a fragmented world: India's data way. India Review. Vol 23. Iss 2. PP 154 - 176. https://doi.org/10.1080/14736489.2024.2324638.

Christopher Kuner. (2023). Protecting EU data outside EU borders under the GDPR. Common Market Law Review. Vol 60. Iss 1. PP 77 – 106. https://doi.org/10.54648/cola2023004.

Chun-Li Ma., Dong-Dong Li., Yalin Li., Yinghao Wu., Song-Yan Ding., Jun Wang., Pei-Yuan Li., Song Zhang, Junjie Chen,

Xiaoxing Zhang, Jia-Yong, Wang, Jin Li., Qiang Li., Zhi-Tong Chen, Lei Zhou, Mei-Sheng Zhao, Yong Zhao. (2023). Quantum-secure fault-tolerant distributed cloud storage system. AIP Advances. Vol 13. Iss 11. 115309. https://doi.org/10.1063/5.0172384.

Debarpita Dutta. (2024). Secure Storage on Cloud using Hybrid Cryptography. International Journal of Advanced Research in Science, Communication and Technology. Vol 4. Iss 1. PP 62 -75. DOI: 10.48175/IJARSCT-18707.

Dharmawan, N., Kasih, D., & Stiawan, D. (2019). Personal data protection and liability of internet service provider: a comparative approach. International Journal of Electrical and Computer Engineering (IJECE). Vol 9. Iss 4. PP 3175 – 3184. https://doi.org/10.11591/IJECE.V9I4.PP3175-3184.

Dieckmann M. A., Beyvers S., Hochmuth J., Rehm A., Förster F., & Goesmann A. (2023). The Aruna Object Storage: A Distributed Multi Cloud Object Storage System for Scientific Data Management. Proceedings of the Conference on Research Data Infrastructure. Vol 1. https://doi.org/10.52825/cordi.v1i.404.

Dimitra Kamarinou, Christopher Millard & Felicity Turton. (2021). Protection of Personal Data in Clouds and Rights of Individuals', in

Christopher Millard (ed.), Cloud Computing Law. 2nd edn Oxford. PP 257 – 293. https://doi.org/10.1093/oso/9780198716662.003.0008.

Dimitrova Diana. (2021). THE NEW STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA BETWEEN EU AND NON-EU COUNTRIES. PROTECTION OF THE PERSONAL DATA AND THE DIGITALIZATION - CHALLENGES AND PERSPECTIVES 2021 CONFERENCE PROCEEDINGS. PP 106 - 115. https://doi.org/10.36997/ppdd2021.106.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). Official Journal L 281, 23/11/1995 P. 0031 – 0050. An official website of the European Union. Available through the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046. It was viewed on: 25/12/2024.

Drechsler L. (2023). Individual Rights in International Personal Data Transfers Under the General Data Protection Regulation.

Review of European Administrative Law. https://doi.org/10.7590/187479823x16800083010347.

Dreyer J., Heitmann S., Erdmann F., Bauer G. & Kray C. (2022). 'Informed' consent in popular location based services and digital sovereignty. Journal of Location Based Services. Vol 16. Iss 4. PP 312 - 342. https://doi.org/10.1080/17489725.2021.2017495.

Dye O., Heo J. & Cankaya E. (2024). Reflection of Federal Data Protection Standards on Cloud Governance. ArXiv, abs/2403.07907. https://doi.org/10.5121/csit.2024.140424.

G. M., et. al. (2021). A Comprehensive Analysis on Efficient Multimedia Storage Mechanism In Public Cloud Environment With Secured Access. Turkish Journal of Computer and Mathematics Education (TURCOMAT). Vol 12. Iss 5. PP 1273 – 1280. doi: 10.1007/978-981-99-3761-5_21.

Gupta Y. (2021). Novel distributed load balancing algorithms in cloud storage. Expert Syst. Appl. Vol 186. 115713. ISSN 0957-4174. https://doi.org/10.1016/J.ESWA.2021.115713.

Harsh Deo Ravi, Tejas Mittal, Gaurav, Sachin Kumar, Anoop Singh & Aadil Feroz. (2024). Secure and Efficient Cloud Storage System with Deduplication and Compression Using Blockchain Technology. International Journal for Research in Applied Science

& Engineering Technology (IJRASET). Vol 45. Iss 98. PP 447 – 455. https://doi.org/10.22214/ijraset.2024.65086.

Hazrat Usman, Iqra Tariq & Bushra Nawaz. (2023). IN THE REALM OF THE MACHINES: AI'S INFLUENCE UPON INTERNATIONAL LAW AND POLICY. JOURNAL OF SOCIAL RESEARCH DEVELOPMENT. Vol 4. Is 2. PP 383 – 399. https://doi.org/10.53664/JSRD/04-02-2023-13-383-399.

Islam M. (2024). Protecting Data Access Liabilities in Cloud Computing. Journal of Artificial Intelligence General science (JAIGS). Vol 3. Iss 1. PP 180 -200. ISSN:3006-4023. https://doi.org/10.60087/jaigs.vol03.issue01.p195.

Islam M. (2024). Protecting Data Access Liabilities in Cloud Computing. Journal of Artificial Intelligence General science (JAIGS). Vol 3. Iss1. PP 180 – 200. ISSN:3006-4023. https://doi.org/10.60087/jaigs.vol03.issue01.p195.

Jim D., Charles C., Edward C., David N. & Ib Holm S. (2005). Formality, Evolution, and Model-driven Software Engineering. Electronic Notes in Theoretical Computer Science. Volume 130. PP 39 – 55. ISSN 1571-0661. https://doi.org/10.1016/j.entcs. 2005.03.004.

Ke T., & Sudhir K. (2022). Privacy Rights and Data Security: GDPR and Personal Data Markets. Management Science. Vol 69. Iss 8. PP 4363-4971. https://doi.org/10.1287/mnsc.2022.4614.

Kitsios F., Chatzidimitriou E. & Kamariotou M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability. Vol 15. 5828. https://doi.org/10.3390/su15075828.

L. Ma, W. Su, B. Wu, B. Yang and X. Jiang. (2022). Joint Emergency Data and Service Evacuation in Cloud Data Centers Against Early Warning Disasters. IEEE Transactions on Network and Service Management. Vol 19. Iss 2. PP 1306 - 1320. https://doi.org/10.1109/tnsm.2022.3147247.

Latha, D.S. (2022). SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY. International Research Journal of Modernization in Engineering Technology and Science. Vol 4. Iss 12. PP 1282 – 1290. https://www.doi.org/10.56726/IRJMETS32383.

Latifian A. (2022). How does cloud computing help businesses to manage big data issues. Kybernetes. Vol 51. Iss 6. PP 1917 - 1948. https://doi.org/10.1108/k-05-2021-0432.

Lee W., Kang M. & Kim S. (2024). Highly VM-Scalable SSD in Cloud Storage Systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. Vol 43. Iss 1. PP 113 - 126. https://doi.org/10.1109/TCAD.2023.3305573.

Li Y., Shi H. & Zhou Y. (2021). The influence of the media on government decisions: Evidence from IPOs in China. Journal of Corporate Finance. Vol 70. PP 102056. https://doi.org/10.1016/J.JCORPFIN.2021.102056.

Loris Belcastro, Fabrizio Marozzo & Paolo Trunfio. (2024). Infrastructures for High-Performance Computing: Cloud Computing. Reference Module in Life Sciences. Elsevier. ISBN: 9780128096338. https://doi.org/10.1016/B978-0-323-95502-7.00005-1.

Luca Bertuzzi & Euractiv. (2021). Cloud development in Europe passes by GDPR compliance. Euractiv. available through the following link: https://www.euractiv.com/sections/tech/. visited on: 28/12/2024.

M. Barati, O. Rana, G. Theodorakopoulos & P. Burnap. (2019). Privacy-Aware Cloud Ecosystems and GDPR Compliance. 2019 7th International Conference on Future Internet of Things and

Cloud (FiCloud). Istanbul. Turkey. PP 117- 124. https://doi.org/10.1109/FiCloud.2019.00024.

Maas Matthijs. (2023). Concepts in advanced AI governance A literature review of key terms and definitions. Legal Priorities Project – AI Foundations Report 3. PP 48 – 50. DOI:10.13140/RG.2.2.26115.68647.

Maha A. Sayal. (2023). Private Storage Cloud for Facilitate the Functions of Organizations. International Journal of Information Technology & Computer Engineering. Vol 3. Iss 6. PP 43 – 51. https://doi.org/10.55529/ijitc.36.43.51.

Mamanazarov S. (2023). DATA OWNERSHIP RIGHTS: FEASIBLE? LEGAL AND TECHNICAL SOLUTIONS. Tsul legal report. https://doi.org/10.51788/tsul.lr.4.4./gvtj6320.

Manju K. Mathai & Juby Mathew. (2024). Chapter Cloud storage (Implementing a third-party public auditing scheme). In Book Research Advances in Network Technologies. Taylor & Francis Group. 1st Edition. PP 18 and beyond. E-ISBN9781003433958.

Marquez J., & Mondragon O. H. (2024). Modelling the Impact of Cloud Storage Heterogeneity on HPC Application Performance. Computation. Vol 12. Iss 7. https://doi.org/10.3390/computation12070150.

Matana, T. (2024). Origin & History of ASP SaaS, PaaS and Cloud Computing. International Journal of Scientific Research and Management (IJSRM). Vol 12. Iss 10. PP 1571 - 1607.https://doi.org/10.18535/ijsrm/v12i10.ec08.

Matthew N. O. Sadiku, Chandra M. M. Kotteti & Janet O. Sadiku. (2024). Cloud Computing Law: An Introduction. International Journal of Trend in Research and Development, Vol 11. Iss 3. P 176. ISSN: 2394-9333

Maxime Lamothe, Yann-Gaël Guéhéneuc, and Weiyi Shang. (2021). A Systematic Review of API Evolution Literature. ACM Comput. Surv. Vol 54. Iss 8. PP 1 - 36. https://doi.org/10.1145/3470133.

Meesala Sravani & Meesala Krishna Murthy. (2023). REDUCTION OF DATA LEAKAGE IN DISTRIBUTED CLOUD STORAGE SYSTEMS USING DISTRIBUTED CLOUD GUARD (DCG). INDIAN JOURNAL OF COMPUTER SCIENCE AND ENGINEERING. Vol 14. Iss 3. PP 444 - 450. ISSN: 0976-5166. https://doi.org/10.21817/indjcse/2023/v14i3/231403014.

Meiditra I., Yuhandri & Sumijan. (2023). ANALISIS DAN PERANCANGAN PRIVATE CLOUD STORAGE MENGGUNAKAN METODE IDS (INTRUSION DETECTION

SYSTEM) DAN IPS (INTRUSION PREVENTION SYSTEM) STUDI KASUS DINAS KOMUNIKASI DAN INFORMATIKA KOTA PADANG PANJANG. Riau Journal of Computer Science (RJOCS). Vol 9. Iss 2. PP 124 – 133. https://doi.org/10.30606/rjocs.v9i2.1781.

Meliá S., Cachero C., Hermida J.M. et al. (2016). Comparison of a textual versus a graphical notation for the maintainability of MDE domain models: an empirical pilot study. Software Qual J Vol 24. PP 709 – 735. https://doi.org/10.1007/s11219-015-9299-x.

Metwally K., Jarray A. & Karmouch A. (2020). A Distributed Auction-based Framework for Scalable IaaS Provisioning in Geo-Data Centers. IEEE Transactions on Cloud Computing. Vol 8. Iss 3. PP 647 - 659. https://doi.org/10.1109/TCC.2018.2808531.

Mondal A.S., Mukhopadhyay A. & Chattopadhyay S. (2022). Machine learning-driven automatic storage space recommendation for object-based cloud storage system. Complex Intell. Syst. Vol 8. PP 489 – 505. https://doi.org/10.1007/s40747-021-00517-4.

Montagnani M. & Cavallo M. (2018). Cybersecurity and Liability in a Big Data World. European Economics: Microeconomics & Industrial Organization eJournal. Vol 11. Iss 2. PP 71 – 99. https://doi.org/10.2139/ssrn.3220475.

N. Manubens, S. D. Smart, T. Quintino & A. Jackson. (2022). Performance Comparison of DAOS and Lustre for Object Data Storage Approaches. 2022 IEEE/ACM International Parallel Data Systems Workshop (PDSW). Dallas. TX. USA. PP 7 - 12. doi: 10.1109/PDSW56643.2022.00007.

Nachiappan R., Calheiros R., Matawie K. & Javadi B. (2023). Optimized Proactive Recovery in Erasure-Coded Cloud Storage Systems. IEEE Access. Vol 11. PP 38226 - 38239. https://doi.org/10.1109/ACCESS.2023.3267106.

Nagappan Mageshkumar, J. Swapna, A. Pandiaraj, R. Rajakumar, Moez Krichen & Vinayakumar Ravi. (2023). Hybrid cloud storage system with enhanced multilayer cryptosystem for secure deduplication in cloud. International Journal of Intelligent Networks. Vol 4. PP 301-309. ISSN 2666-6030. https://doi.org/10.1016/j.ijin.2023.11.001.

Nikkhah H. & Grover V. (2022). An Empirical Investigation of Company Response to Data Breaches. MIS Quarterly. Vol 46. Iss 4. PP 2163 - 2196. https://doi.org/10.25300/misq/2022/16609.

Noopur Malse, Aditya Lad, Atharv Mandpe & Nishant Lanjewar. (2024). Developing a Secure Private Cloud Storage System. International Journal for Research in Applied Science &

Engineering Technology (IJRASET). Vol 12. Iss XI. PP 1419 – 1425. https://doi.org/10.22214/ijraset.2024.65348.

P. Yang N. Xiong & J. Ren. Data Security and Privacy Protection for Cloud Storage: A Survey. in IEEE Access. Vol 8. PP 131723 - 131740, 2020, doi: 10.1109/ACCESS.2020.3009876.

Patnaik S., Garikapati K., Dash L., Bhattacharya R., & Mohapatra A. (2024). Safeguarding Patient Privacy: Exploring Data Protection in E-Health Laws: A Cross-Country Analysis. EAI Endorsed Transactions on Pervasive Health and Technology. Vol 10. https://doi.org/10.4108/eetpht.10.5583.

Petrosyan D. & Astsatryan H. (2022). Serverless High-Performance Computing over Cloud. Cybernetics and Information Technologies. Sciendo. Vol 22. Iss 3. PP 82 - 92. https://doi.org/10.2478/cait-2022-0029.

Plewnia C. & Lichter H. (2023). Cross-provider Cloud Cost Calculation. 13th International Workshop on Enterprise Modeling and Information Systems Architectures (EMISA 2023). CEUR Workshop Proceedings; 3397. https://ceur-ws.org/Vol-3397/sci3.pdf.

Privacy Act. (N. D.). The Privacy Act of 1974, as amended, provides safeguards against unwarranted invasions of privacy by

establishing a code of "fair information practices". U.S. Department of the Treasury. Available through the following link: https://home.treasury.gov/footer/privacy-act. It was viewed on: 25/12/2024.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. (2021). EUROPEAN COMMISSION. Available through the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206. It was viewed on: 27/12/2024.

Q. Dong J. Tang S. Dang G. Chen & J. A. Chambers. (2023). Blockchain-Assisted Reputation Mechanism for Distributed Cloud Storage," in IEEE Systems Journal. Vol 17. Iss 4. PP 6334 – 6345. doi: 10.1109/JSYST.2023.3277194.

R. Kanna, D. Lakshmi, P. Muneeshwari, G. M. Valantina & R. Suguna. (2024). Enhancing Enterprise Data Management with Secure and Scalable Cloud Storage Solutions. 2024 Second International Conference on Advances in Information Technology

(ICAIT), Chikkamagaluru, Karnataka. India. PP 1 – 6. doi: 10.1109/ICAIT61638.2024.10690776.

Rangaswamy K., Gurusamy M., & Vijayakumar P. (2020). An Efficient Cloud Data Center Allocation to the Source of Requests. J. Organ. End User Comput. Vol 32. Iss 3. PP 23 - 36. https://doi.org/10.4018/joeuc.2020070103.

Ranjan, R. (2014). The Cloud Interoperability Challenge. IEEE Cloud Computing. Vol 1. Iss 2. PP 20 - 24. https://doi.org/10.1109/MCC.2014.41.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). OJ L 119, 4.5.2016, p. 1–88 (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV). available through the following link: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Robol M., Breaux T., Paja E. & Giorgini P. (2022). Consent Verification Monitoring. ACM Transactions on Software Engineering and Methodology. Vol 32. Iss 1. PP 1 - 33. https://doi.org/10.1145/3490754.

S. HR & T. S. (2021). A Hybrid Cloud Approach for Efficient Data Storage and Security. 2021 6th International Conference on Communication and Electronics Systems (ICCES). Coimbatre, India. PP 1072 – 1076. doi: 10.1109/ICCES51350.2021.9488938.

S. Pearson & M. Casassa-Mont. (2011). Sticky Policies: An Approach for Managing Privacy across Multiple Parties. Computer. Vol. 44. Iss 9. PP 60 - 68. https://doi.org/10.1109/MC.2011.225.

Sambaiah. G, E. Kiran Kumar. (2020). Imperative Requirements for Data Security in Cloud Computing. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Vol 9. Iss 7. https://doi.org/10.17577/ijertv9is070455.

Singh, U., Tiwari, A., & Sharma, S. (2023). DATA SECURITY IN CLOUD COMPUTING. journalofcardiovasculardiseaseresearch. Vol 12. Iss 2. PP 696 – 705. https://doi.org/10.48047/jcdr.2021.12.02.91.

Soltani S., Martin P. & Elgazzar K. (2018). A hybrid approach to automatic IaaS service selection. Journal of Cloud Computing. Vol 7. Article number: 12. https://doi.org/10.1186/s13677-018-0113-8.

Susi M. (2020). The Right to Be Forgotten. In A. von Arnauld K. von der Decken & M. Susi (Eds.), The Cambridge Handbook of New Human Rights: Recognition. Novelty. Rhetoric. Chapter.

Cambridge: Cambridge University Press. PP 287 – 299. https://doi.org/10.1017/9781108676106.023.

Tak, B., Tang, C., Chang, R., & Seo, E. (2021). Block-Level Storage Caching for Hypervisor-Based Cloud Nodes. IEEE Access. Vol 9. PP 88724 - 88736. https://doi.org/10.1109/ACCESS.2021.3090308.

Truong N., Sun K., Lee G. & Guo Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security. Vol 15. https://doi.org/10.1109/TIFS.2019.2948287.

Truong N., Sun K., Lee G. & Guo Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. IEEE Transactions on Information Forensics and Security. Vol 15. https://doi.org/10.1109/TIFS.2019.2948287.

Tsai W., Bai X. & Huang Y. (2014). Software-as-a-service (SaaS): perspectives and challenges. Science China Information Sciences. Vol 57. PP 1 - 15. https://doi.org/10.1007/s11432-013-5050-z.

V.G, P.A. (2024). SecureLaw Portal: Empowering Citizens with Transparent Legal Records via Blockchain and Cloud eVault. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN

ENGINEERING AND MANAGEMENT. Vol 8. Iss 12. ISSN: 2582-3930.

Wang Y. (2021). Security-driven distributed platforms for intellectual property resource provision - a case study of TSITE IP. J Cloud Comp. Vol 10. Iss 56. https://doi.org/10.1186/s13677-021-00274-2.

What is GDPR, the EU's new data protection law? (N. D.). GDPR.EU. Available through the following link: https://gdpr.eu/what-is-gdpr/. It was viewed on: 25/12/2024.

Wiegand E., Liu A. & Sedovic S. (2024). Algorithmic Accountability for Record Linkage. International Journal of Population Data Science. Vol 9. Iss 5. doi: 10.23889/ijpds.v9i5.2854.

Yang P., Xiong N. & Ren J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access. Vol 8. PP 131723 - 131740. https://doi.org/10.1109/ACCESS.2020.3009876.

Yang Z., Wang W. & Huang Y. (2017). Ensuring reliable logging for data accountability in untrusted cloud storage. 2017 IEEE International Conference on Communications (ICC). PP 1 - 6. https://doi.org/10.1109/ICC.2017.7997109.

Yaser Mansouri, Adel Nadjaran Toosi, & Rajkumar Buyya. (2017). Data Storage Management in Cloud Environments: Taxonomy, Survey, and Future Directions. ACM Computing Surveys (CSUR). Vol 50. Iss 6. PP 1 – 50. https://doi.org/10.1145/3136623.

Yogesh Gupta. (2021). Novel distributed load balancing algorithms in cloud storage. Expert Systems with Applications. Vol 186. 115713. ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2021.115713.

Yu. S. Kharitonova. (2023). Legal Means of Providing the Principle of Transparency of the Artificial Intelligence. Journal of Digital Technologies and Law. Vol 1. Iss 2. PP 337 – 358. https://doi.org/10.21202/jdtl.2023.14.

Yuan D., Cui L., Li W., Liu X. & Yang Y. (2018). An Algorithm for Finding the Minimum Cost of Storing and Regenerating Datasets in Multiple Clouds. IEEE Transactions on Cloud Computing. Vol 6. Iss 2. PP 519 - 531. https://doi.org/10.1109/TCC.2015.2491920.

Zephrina C. & J Bhuvana. (2024). Revolutionizing Cloud Storage Security: Searchable Public-Key Encryption. International Journal of Innovative Research in Computer and Communication

Engineering. Vol 12. Iss 3. PP 1883 – 1888. https://doi.org/10.15680/ijircce.2024.1203085.

Zhang W. & Zhang Y. (2023). Enigma of Relationship between Digital Economy and Intellectual Property Rights: Reflections on Innovation in Digital Economy Represented by Cloud Computing. EAI Endorsed Transactions on Scalable Information Systems. Vol 10. Iss 6. https://doi.org/10.4108/eetsis.3946.

Zhao Y., Qu Y., Xiang Y. & Gao L. (2022). A Comprehensive Survey on Edge Data Integrity Verification: Fundamentals and Future Trends. ArXiv, abs/2210.10978. https://doi.org/10.48550/arXiv.2210.10978.

Zhu J. J., Tuo L., You Y., Fei Q. & Thomson M. (2024). A Preemptive and Curative Solution to Mitigate Data Breaches: Corporate Social Responsibility as a Double Layer of Protection. Journal of Marketing Research. Vol 61. Iss 4. PP 778 - 801. https://doi.org/10.1177/00222437231218969.

Zichichi M., Ferretti S. & D'angelo G. (2020). On the Efficiency of Decentralized File Storage for Personal Information Management Systems. 2020 IEEE Symposium on Computers and Communications (ISCC). PP 1 - 6. https://api.semanticscholar.org/CorpusID:220381264.

Zou Y. & Schaub F. (2019). Beyond Mandatory: Making Data Breach Notifications Useful for Consumers. IEEE Security & Privacy. Vol 17. Iss 2. PP 67 - 72. https://doi.org/10.1109/MSEC.2019.2897834.

Zuo L. & Yun D. (2024). Optimal Balancing of Data Transfer Time and Cost in High-Performance Networks. 2024 International Conference on Computing, Networking and Communications (ICNC). PP 60 - 64. https://doi.org/10.1109/ICNC59896.2024.10556371.

Д. М. Бєлов, М. В. Бєлова & О. Т. Горнило. (2024). Право людини на забуття. Науковий вісник Ужгородського національного університету. Серія: Право. Том 2 № 81. PP 57 – 63. https://doi.org/10.24144/2307-3322.2024.81.2.9.

Ляпунов Б.А. (2019). Приватность личности: понятие, сущность и правовая природа. Актуальные проблемы российского права. Vol 2. PP 33 - 42. https://doi.org/10.17803/1994-1471.2019.99.2.033-042.

Меньшиков П.В. & Михина Л. К. (2022). Система противодействия угрозам информационной безопасности КНР// Вестник Забайкальского государственного

университета. Т 28. № 1. PP 124 - 139. DOI: 10.21209/2227-9245-2022-28-1-124-139.

Н.Т. Головацький. (2024). Питання захисту персональних даних при використанні хмарних технологій. Аналітично-порівняльне правознавство. № 5. PP 460 – 466. https://doi.org/10.24144/2788-6018.2024.05.72.