جامعة الأزهر
كلية الشريعة والقانون بدمنهور

مـجلة البحوث
الفقهية والقانونية

مجلة علمية محكمّة
تصدرها كلية الشريعة والقانون بدمنهور

بحث مستل من
العدد الخمسين ـ "إصدار يوليو ٢٠٢٥م ـ ١٤٤٧هـ"

النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي: دراسة تحليلية مقارنة

Legal Disputes Arising from the Use of Cloud Storage Services A Comparative Analytical Study

الدكتـــور
بدر سعد العتيبي
محامي محكمة التمييز والمحكمة الدستورية
وعضو في جمعية المحامين الكويتية

مجلـة البحـوث الفقهيــة والقانونيــة
مجلة علمية عالمية متخصصة ومُحكمة
من السادة أعضاء اللجنة العلمية الدائمة والقارئة
في كافة التخصصات والأقسام العلمية بجامعة الأزهر

المجلة مدرجة في الكشاف العربي للإستشهادات المرجعية ARABIC CITATION INDEX
على Clarivate Web of Science
المجلة مكشّفة في قاعدة معلومات العلوم الإسلامية والقانونية من ضمن قواعد بيانات دار المنظومة
المجلة حاصلة على تقييم ٧ من ٧ من المجلس الأعلى للجامعات
المجلة حاصلة على المرتبة الأولى على المستوى العربي في تخصص الدراسات الإسلامية
وتصنيف Q2 في تخصص القانون حسب تقييم معامل "ارسيف Arcif" العالمية
المجلة حاصلة على تقييم ٨ من المكتبة الرقمية لجامعة الأزهر

رقم الإيداع
٦٣٥٩

الترقيم الدولي
(ISSN-P): (1110-3779) - (ISSN-O): (2636-2805)

للتواصل مع المجلة
+201221067852
journal.sha.law.dam@azhar.edu.eg

موقع المجلة على بنك المعرفة المصري
https://jlr.journals.ekb.eg

التاريخ: 2024/10/20

الرقم: L24/0260 ARCIF

سعادة أ. د. رئيس تحرير مجلة البحوث الفقهية و القانونية المحترم

جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر

تحية طيبة وبعد،،،

يسر **معامل التأثير والاستشهادات المرجعية للمجلات العلمية العربية (ارسيف – ARCIF)**، أحد مبادرات قاعدة بيانات "**معرفة**" للإنتاج والمحتوى العلمي، إعلامكم بأنه قد **أطلق التقرير السنوي التاسع للمجلات للعام 2024.**

يخضع معامل التأثير "ارسيف Arcif" لإشراف "مجلس الإشراف والتنسيق" الذي يتكون من ممثلين لعدة جهات عربية ودولية: (مكتب اليونيسكو الإقليمي للتربية في الدول العربية ببيروت، لجنة الأمم المتحدة لغرب آسيا (الإسكوا)، مكتبة الاسكندرية، قاعدة بيانات معرفة). بالإضافة للجنة علمية من خبراء وأكاديميين ذوي سمعة علمية رائدة من عدة دول عربية وبريطانيا.

ومن الجدير بالذكر بأن معامل "**ارسيف Arcif**" قام بالعمل على فحص ودراسة بيانات ما يزيد عن (**5000**) عنوان مجلة عربية علمية أو بحثية في مختلف التخصصات، والصادرة عن أكثر من (**1500**) هيئة علمية أو بحثية في العالم العربي. ونجح منها (**1201**) مجلة علمية فقط لتكون معتمدة ضمن المعايير العالمية لمعامل "**ارسيف Arcif**" في تقرير **عام 2024.**

ويسرنا تهنئتكم وإعلامكم بأن **مجلة البحوث الفقهية و القانونية** الصادرة عن **جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر، قد نجحت في تحقيق معايير اعتماد معامل "ارسيف Arcif"** المتوافقة مع المعايير العالمية، والتي يبلغ عددها (**32**) **معياراً**، وللاطلاع على هذه المعايير يمكنكم الدخول إلى الرابط التالي: http://e-marefa.net/arcif/criteria/

وكان **معامل "ارسيف Arcif" العام** لمجلتكم لسنة 2024 (**0.3827**). ونهنئكم بحصول المجلة على:

- **المرتبة الأولى في تخصص الدراسات الإسلامية من إجمالي عدد المجلات (103)** على المستوى العربي، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.082**). كما صُنفت مجلتكم في هذا التخصص ضمن الفئة (**Q1**) وهي الفئة العليا .
- كما صُنفت مجلتكم في **تخصص القانون** من **إجمالي عدد المجلات (114)** على المستوى العربي ضمن الفئة (**Q2**) وهي الفئة الوسطى المرتفعة ، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.24**).

راجين العلم أن حصول أي مجلة ما على مرتبة ضمن الأعلى (10) مجلات في **تقرير معامل "ارسيف" لعام 2024** في أي تخصص، **لا يعني حصول** المجلة بشكل تلقائي على تصنيف مرتفع كتصنيف فئة Q1 أو Q2، حيث يرتبط ذلك بإجمالي قيمة النقاط التي حصلت عليها من **المعايير الخمسة المعتمدة لتصنيف مجلات تقرير "ارسيف" (للعام 2024) إلى فئات في مختلف التخصصات**، ويمكن الاطلاع على هذه المعايير الخمسة من خلال الدخول إلى الرابط: http://e-marefa.net/arcif/

وبإمكانكم الإعلان عن هذه النتيجة سواء على موقعكم الإلكتروني، أو على مواقع التواصل الاجتماعي، وكذلك الإشارة في النسخة الورقية لمجلتكم إلى معامل "**ارسيف Arcif**" الخاص بمجلتكم.

ختاماً، في حال رغبتكم الحصول على شهادة رسمية إلكترونية خاصة بنجاحكم في معامل "**ارسيف**"، نرجو التواصل معنا مشكورين.

وتفضلوا بقبول فائق الاحترام والتقدير

أ.د. سامي الخزندار

رئيس مبادرة معامل التأثير

" ارسيف Arcif"

النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي: دراسة تحليلية مقارنة

Legal Disputes Arising from the Use of Cloud Storage Services A Comparative Analytical Study

الدكتـــــور

بدر سعد العتيبي

محامي محكمة التمييز والمحكمة الدستورية

وعضو في جمعية المحامين الكويتية

النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي
دراسة تحليلية مقارنة

بدر سعد العتيبي

قسم القانون المدني، كلية الحقوق، جامعة المنوفية، جمهورية مصر العربية.

البريد الإلكتروني: baderlaw2@gmail.com

ملخص البحث:

تُقدم هذه الدراسة تحليلًا معمقًا للنزاعات القانونية الناشئة عن الاستخدام المتزايد لخدمات التخزين السحابي، من خلال تحليل الإطار القانوني، واستعراض أهم الإشكاليات التي تثيرها في مختلف الأنظمة القانونية. وتهدف الدراسة إلى بيان مدى كفاية القوانين الحالية في تنظيم العلاقة بين مزودي هذه الخدمات ومستخدميها، وتحليل أوجه القصور التي قد تؤدي إلى نشوء منازعات قضائية.

وتُبرز الدراسة أبرز المشكلات القانونية، مثل تحديد الاختصاص القضائي في النزاعات العابرة للحدود، والمسؤولية القانونية لمزودي خدمات التخزين السحابي عند فقدان أو اختراق البيانات، وكذلك إشكالية حماية خصوصية المستخدمين وحقوقهم الرقمية. كما تتطرق إلى أحكام العقود الإلكترونية المبرمة بين الأطراف، وإشكاليات الإثبات الرقمي عند نشوء المنازعات.

وتعتمد الدراسة على منهج مقارن بين القوانين والتشريعات ذات الصلة في بعض الأنظمة القانونية، مثل القانون الأوروبي، والقانون الأمريكي، والقانون المصري، بهدف الوقوف على أوجه التشابه والاختلاف في تنظيم هذه الخدمات وحماية حقوق المستخدمين.

وخلصت الدراسة إلى ضرورة تطوير الإطار التشريعي الوطني والدولي، بما يضمن حماية حقوق المستخدمين ومزودي الخدمات على حد سواء، ويدعم مبادئ العدالة الرقمية. كما توصي الدراسة بضرورة تعزيز التعاون الدولي لوضع قواعد موحدة أو اتفاقيات دولية لمعالجة النزاعات الناشئة عن خدمات التخزين السحابي، بما يحقق التوازن بين متطلبات الابتكار وحماية الحقوق القانونية.

كلمات مفتاحية: الحوسبة السحابية، حماية البيانات من السرقة، الخصوصية، الأمن السيبراني، الاختصاص القضائي، التحكيم الإلكتروني.

Legal Disputes Arising from the Use of Cloud Storage Services
A Comparative Analytical Study

Badar Saad Al-Otaibi
Department of Civil Law, Faculty of Law, Menoufia University, Egypt.
E-mail: baderlaw2@gmail.com

Abstract:

This study offers an in-depth analysis of the legal disputes arising from the increasing use of cloud storage services. It examines the legal framework governing such disputes and identifies the key issues that arise in various legal systems. The study aims to assess the adequacy of current laws in regulating the relationship between cloud service providers and their users, while analyzing potential gaps that may lead to legal disputes.

The study highlights the most significant legal issues, such as determining jurisdiction in cross-border disputes, the legal liability of cloud storage providers in cases of data loss or breaches, as well as challenges related to the protection of users' privacy and digital rights. It also addresses the provisions of electronic contracts concluded between the parties and the evidentiary challenges of digital evidence in the event of disputes.

The study adopts a comparative approach, examining relevant laws and regulations in selected legal systems, such as European law, American law, and Egyptian law. This comparative analysis seeks to identify the similarities and differences in regulating these services and in safeguarding users' rights.

The study concludes that it is necessary to develop national and international legislative frameworks to ensure the protection of both users and service providers, while supporting the principles of digital justice. Furthermore, it recommends enhancing international cooperation to establish unified rules or international agreements to address disputes arising from cloud storage services, thereby striking a balance between fostering innovation and protecting legal rights.

Keywords: Cloud Computing, Data Protection Against Theft, Privacy, Cybersecurity, Jurisdiction, Electronic Arbitration.

المقدمة:

تُعدّ خدمات التخزين السحابي إحدى الركائز الأساسية للتحول الرقمي، إذ تتيح تخزين البيانات وإدارتها بكفاءة عبر الشبكة العنكبوتية. موفرةً حلولًا مرنة وفعّالة للأفراد والمؤسسات على حدّ سواء. ومع التوسّع المتسارع في اعتماد هذه الخدمات، برزت تحدّيات قانونية معقّدة تتعلّق بحماية البيانات، الخصوصية، الأمن السيبراني، والمسؤولية القانونية. غير أنّ هذا التطور قد أفضى إلى ظهور تحديات قانونية معقدة تتعلق بالنزاعات الناشئة عن استخدام هذه الخدمات.

فخدمات التخزين السحابي من بين التطبيقات الأكثر شيوعًا وانتشارًا في هذا المجال، لما توفره من مزايا تتعلق بالكفاءة، والمرونة، وخفض التكاليف، وإمكانية الوصول إلى البيانات من أي مكان وفي أي وقت.

غير أن هذا التحول لم يخلُ من إشكاليات قانونية مستجدة، إذ نشأت عن استخدام هذه الخدمات نزاعات قانونية معقدة تتصل بطبيعة العلاقة التعاقدية بين المستخدم ومزوّد الخدمة، ومدى انطباق قواعد المسؤولية المدنية، وحدود الالتزامات القانونية للطرفين. كما تطرح بيئة التخزين السحابي إشكالات تتعلق بالاختصاص القضائي، وتنازع القوانين، ونطاق حماية الخصوصية والبيانات الشخصية، خاصة في السياق العابر للحدود، إذ قد تُخزن البيانات في مواقع متعددة تقع خارج النطاق القانوني للدولة الأم.

فضلًا عن التحديات المرتبطة بإبرام العقود الإلكترونية وتفسيرها في هذا السياق الافتراضي. وبات من الضروري تحليل النزاعات الناشئة واستجلاء أوجه القصور في الأطر القانونية التقليدية عند التعامل مع هذه المستجدات التقنية.

وتزداد أهمية معالجة هذه القضايا في ظل التباين التشريعي بين النظم القانونية، والقصور الواضح في بعض الأطر التنظيمية القائمة، مما يخلق فراغًا قانونيًّا يُصعّب من حسم النزاعات المتعلقة بفقدان البيانات، أو اختراقها، أو إساءة استخدامها، فضلًا عن الشروط التعاقدية الجائرة التي قد تُدرج من قِبل مزوّدي الخدمات دون تفاوض حقيقي.

من هذا المنطلق، تسعى هذه الدراسة إلى تقديم تحليل معمق ومقارن للنزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي، من خلال استقراء عدد من النماذج التشريعية المتقدمة، واستعراض الاتجاهات القضائية ذات الصلة، بهدف الوصول إلى رؤية قانونية متكاملة تمُكّن من تنظيم هذه العلاقة التقنية–التعاقدية على نحو يحقق العدالة وحماية الحقوق الرقمية للأطراف المعنية، ويواكب تطورات الفضاء السيبراني.

أهمية الدراسة:

تتناول الدراسة قضية محورية تتعلق بالنزاعات القانونية المترتبة على استخدام خدمات التخزين السحابي، التي تشكل ركيزة أساسية في العصر الرقمي. كما تشكل جزءًا أساسيًّا من البنية التحتية للمؤسسات العامة والخاصة على حد سواء، فضلًا عن استخدامها الواسع من قبل الأفراد. وفي ظل الاعتماد المتزايد على هذه الخدمات، برزت الحاجة الملحّة إلى معالجة التحديات القانونية التي ترافقها، ولا سيما في مجالات المسؤولية المدنية، وحماية الخصوصية، ونقل البيانات عبر الحدود، وإثبات العقود المبرمة إلكترونيًّا.

كما تمثل ندرة الأبحاث العربية المتخصصة التي تتناول النزاعات القانونية الناجمة عن استخدام التخزين السحابي بأسلوب مقارن وتحليلي، وهو ما تسعى هذه الدراسة إلى معالجته من خلال تسليط الضوء على أوجه القصور في التشريعات الحالية، واستعراض النماذج القانونية المقارنة، بغرض الوصول إلى رؤية متكاملة تسهم في تطوير منظومة قانونية فعالة ومواكبة للتطورات التقنية.

وتتجلّى أهمية هذه الدراسة في بعدها العملي، إذ إنها توفّر مرجعًا مهمًّا للمشرّعين، والقضاة، والمحامين، ومزودي خدمات الحوسبة السحابية، من خلال تحليل إشكاليات واقعية واستنباط حلول قانونية قابلة للتطبيق، مما يُسهم في تقليل حجم النزاعات المستقبلية وتحقيق التوازن بين مصالح المستخدمين ومزودي الخدمة.

وإلى جانب ذلك، فإن تناول الإشكالات القانونية المرتبطة بخدمات التخزين السحابي يسهم بشكل مباشر في دعم منظومة الأمن السيبراني، من خلال تعزيز الإطار القانوني الناظم لحماية البيانات والمعاملات الرقمية، بما يرسّخ الثقة لدى الأفراد والمؤسسات في استخدام التقنيات السحابية ويضمن استدامة التحول الرقمي الآمن. ومن ثم، تُعدّ هذه الدراسة إسهاما فاعلا في بناء بيئة رقمية قائمة على الأمان القانوني، والشفافية، وحوكمة البيانات.

أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف المتكاملة التي تركز على النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي، وذلك من خلال نهج تحليلي مقارن. وتتمثل الأهداف فيما يلي:

١- **استقصاء النزاعات القانونية**: تحديد وتصنيف أبرز النزاعات القانونية المرتبطة بخدمات التخزين السحابي، مثل قضايا الخصوصية، حماية البيانات، خرق العقود، والاختصاص القضائي.

٢- **تحليل الأطر القانونية**: دراسة الأنظمة القانونية المنظمة لخدمات التخزين السحابي في سياقات تشريعية متنوعة، لفهم كيفية معالجة هذه النزاعات.

٣- **المقارنة بين التجارب القانونية**: إجراء تحليل مقارن بين الأنظمة القانونية المختلفة للكشف عن نقاط القوة والضعف في التعامل مع التحديات القانونية لهذه الخدمات.

٤- **تقديم توصيات تشريعية**: اقتراح حلول وسياسات قانونية تعزز من فعالية الأطر التشريعية، بما يحقق التوازن بين دعم الابتكار التكنولوجي وحماية حقوق الأفراد والمؤسسات.

٥- **تعزيز الوعي القانوني**: توفير مرجعية علمية تسهم في رفع مستوى الوعي لدى المستخدمين، المزودين، والمشرعين بأبعاد النزاعات القانونية وسبل الوقاية منها.

من خلال هذه الأهداف، تسعى الدراسة إلى تقديم إسهام نوعي في تطوير الأطر القانونية المتعلقة بخدمات التخزين السحابي، بما يدعم الاقتصاد الرقمي ويحد من المخاطر القانونية.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في التعقيدات القانونية الناشئة عن استخدام خدمات التخزين السحابي، التي تتجلى في تزايد النزاعات القانونية المرتبطة بها، مثل انتهاكات الخصوصية، فقدان البيانات، خرق العقود، والتضارب في الاختصاص القضائي بين الأنظمة القانونية المختلفة. يفاقم هذه المشكلة غياب التناسق في التشريعات المنظمة للخدمات السحابية عبر الدول، مما يؤدي إلى تحديات في حماية حقوق المستخدمين وتحديد المسؤوليات القانونية لمزودي الخدمات.

كما أن الطابع العابر للحدود لهذه الخدمات يثير إشكاليات متعلقة بتطبيق القوانين المحلية على بيانات مخزنة في مواقع جغرافية مختلفة. وفي ظل الاعتماد المتزايد على التخزين السحابي في القطاعات الحيوية كالصحة والمالية، تبرز الحاجة الملحة لدراسة هذه النزاعات بشكل تحليلي مقارن، لفهم طبيعتها، تحديد أسبابها، واقتراح حلول قانونية فعّالة. تسعى الدراسة إلى الإجابة عن السؤال الرئيس: كيف يمكن للأطر القانونية المعاصرة معالجة النزاعات الناشئة عن خدمات التخزين السحابي بفعالية، وما هي أفضل الممارسات التي يمكن تبنيها لتحقيق التوازن بين الابتكار التكنولوجي وحماية الحقوق؟

إشكالية الدراسة وتساؤلاتها:

في ظل التحول الرقمي المتسارع، باتت خدمات التخزين السحابي أداة أساسية تعتمد عليها المؤسسات والأفراد لحفظ البيانات وتبادلها وتشغيل البرمجيات عن بُعد. إلا أن هذا التطور التقني، على الرغم من مزاياه، أفرز جملة من التحديات القانونية التي لا تزال محل جدل واسع في الفقه والقضاء، خصوصًا بسبب الطابع اللامادي والعابر للحدود لهذه الخدمات، الأمر الذي يثير تساؤلات حول مدى كفاية الأطر القانونية التقليدية في مواكبة هذا النوع من العلاقات الرقمية.

وتتمثّل إشكالية الدراسة في وجود فراغ أو قصور تشريعي واضح في العديد من الأنظمة القانونية، لا سيما في الدول العربية، بشأن تنظيم الجوانب القانونية المرتبطة بخدمات التخزين السحابي، وتحديد المسؤوليات القانونية الناشئة عن النزاعات المرتبطة بها، سواء تعلّقت بانتهاك الخصوصية، أو ضياع البيانات، أو خرق العقود، أو صعوبة تحديد الاختصاص القضائي والقانون الواجب التطبيق في حال حدوث نزاع.

كما تبرز الإشكالية في قصور التشريعات الوطنية في عدد من الدول، ومنها بعض الدول العربية، عن مواكبة التطورات التقنية المتسارعة، الأمر الذي يؤدي إلى وجود فراغ قانوني أو تضارب في المعايير، مما ينعكس سلبًا على حماية حقوق المستخدمين، ويؤثر على موثوقية بيئة التخزين السحابي ويقوّض من فرص الاعتماد الآمن عليها. ومن هنا، تنطلق هذه الدراسة لمحاولة الإجابة عن السؤال الرئيس الآتي:

-إلى أي مدى تُوفِّر الأطر القانونية الحالية حماية فعالة للأطراف المتعاملة مع خدمات التخزين السحابي؟

-وما سُبل تطوير تلك الأطر بما يكفل تحقيق التوازن بين الابتكار التقني وضمان الحقوق القانونية في البيئة الرقمي؟

وانطلاقًا من السؤال الرئيس، تسعى الدراسة إلى الإجابة على التساؤلات والفرعية التالية:

-ما أبرز أنواع النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي، وما هي أسبابها الرئيسة؟

-كيف تتناول الأطر القانونية المختلفة (محلية ودولية) هذه النزاعات، وما هي الفروقات بينها؟

-ما مدى فعالية التشريعات الحالية في حماية حقوق المستخدمين وتحديد مسؤوليات مزودي خدمات التخزين السحابي؟

-ما التحديات التي تواجه تطبيق القوانين على الخدمات السحابية العابرة للحدود، وكيف يمكن معالجتها؟

-ما أفضل الممارسات القانونية التي يمكن تبنيها لتقليل النزاعات القانونية المرتبطة بالتخزين السحابي وتعزيز الثقة في هذه الخدمات؟

ومن خلال الإجابة عن هذه التساؤلات، تسعى الدراسة إلى تقديم رؤية متكاملة تسهم في تطوير الأطر القانونية، وتعزز من قدرة الأنظمة القانونية على مواجهة التحديات المستجدة في الاقتصاد الرقمي.

منهجية الدراسة:

تعتمد هذه الدراسة على مزيج من المناهج القانونية المناسبة لطبيعة الموضوع، بهدف تحليل الإشكاليات المرتبطة بالنزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي، واستجلاء أوجه القصور والاختلاف في الأطر التنظيمية، واقتراح حلول قانونية عملية. وتتمثل منهجية الدراسة فيما يلي:

١ـ **المنهج التحليلي (الوصفي)**: ويُستخدم لتحليل المفاهيم الأساسية المرتبطة بخدمات التخزين السحابي، وبيان طبيعتها التقنية والقانونية، واستعراض الجوانب التنظيمية المؤثرة على العلاقة بين مزود الخدمة والمستخدم، إلى جانب توصيف صور النزاعات القانونية الناشئة عن تلك الخدمات.

٢ـ **المنهج المقارن**: يُستخدم لمقارنة النظم القانونية المختلفة في تنظيم النزاعات المتعلقة بخدمات التخزين السحابي، وذلك من خلال دراسة تشريعات مختارة (مثل التشريع الأوروبي، وبعض النماذج من الدول العربية مثل مصر أو الإمارات)، لاستخلاص أوجه التباين والتقارب بين هذه النظم، والوقوف على أفضل الممارسات التي يمكن الاستفادة منها لتطوير التشريعات العربية.

تتيح هذه المنهجية إطارًا منظمًا لدراسة النزاعات القانونية بشكل شامل، مع ضمان تقديم نتائج وتوصيات ذات فاعلية، يمكن أن تسهم في تطوير الأطر القانونية المنظمة لخدمات التخزين السحابي.

خطة الدراسة:

لضمان تنظيم الدراسة بشكل منهجي، وتحقيق أهدافها في استقصاء النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي يتبع الباحث التقسيم التالي للدراسة:

المبحث الأول: ماهية التخزين السحابي.

المطلب الأول: مفهوم التخزين السحابي أنواعه.

المطلب الثاني: خصائص التخزين السحابي.

المبحث الثاني: التحديات القانونية المرتبطة بالخدمات السحابية.

المطلب الأول: طبيعة النزاعات القانونية في بيئات التخزين السحابي.

المطلب الثاني: تحليل للمنهج القانوني المرتبط بالخدمات السحابية.

المبحث الثالث: القانون الواجب التطبيق وطرق فض نزاعات التخزين السحابي.

المطلب الأول: القانون الواجب التطبيق على نزاعات التخزين السحابي

المطلب الثاني: طرق فض النزاعات المتعلقة بالحوسبة السحابية.

المبحث الأول
ماهية التخزين السحابي

تستمر المستندات، سواء المادية أو الرقمية، في التزايد بمرور الوقت، مما يستلزم توفير مساحات تخزين موسعة تتناسب مع طبيعتها. تختلف متطلبات التخزين بين المستندات المادية، التي تعتمد على أرفف مادية وبنية تحتية داعمة، والمستندات الرقمية، التي تتطلب مساحات تخزين افتراضية. تتطلب المستندات المادية مساحة تخزين فيزيائية، بينما تعتمد المستندات الرقمية على سعة تخزين البيانات الإلكترونية[١].

في المراحل المبكرة لتطور التخزين الرقمي، ظهرت وسائط مثل محركات الأقراص الصلبة، وأقراص CD/DVD، وغيرها من الأجهزة الإلكترونية. ومع ذلك، تواجه هذه الوسائط قيودًا جوهرية، أبرزها محدودية سعة التخزين وضعف الأمان أمام التهديدات السيبرانية، مثل الهجمات البرمجية الضارة، التي أصبحت تحدث بشكل متكرر. وقد أبلغ موظفو مكتب فرع منطقة نجيمبلاك بويولالي عن هذه التحديات، مما يعكس الحاجة الملحة إلى حلول تخزين أكثر كفاءة وأمانًا لتلبية متطلبات إدارة المستندات الرقمية في بيئات العمل الحديثة[٢].

هذا الواقع يُبرز أهمية تطوير استراتيجيات تخزين مبتكرة، مثل الحوسبة السحابية، التي توفر سعة تخزين مرنة وآليات أمان متقدمة، لتلبية الاحتياجات المتزايدة للمؤسسات في إدارة بياناتها بفعالية واستدامة.

ويؤدي فصل البيانات في أجهزة الحاسوب الشخصية إلى زيادة حاجة الموظفين إلى وسائط تخزين إضافية، مثل أقراص الفلاش، لتسهيل تبادل البيانات. ومع ذلك، يُقدم التخزين السحابي، المستند إلى تقنيات الحوسبة السحابية، بديلًا فعالًا يعتمد على شبكة الإنترنت لإدارة ملفات المستندات وفقًا لاحتياجات المستخدمين. يوفر التخزين السحابي مزايا متعددة، تشمل سهولة التثبيت، مزامنة البيانات عبر أجهزة متنوعة (مثل أجهزة الحاسوب والهواتف الذكية)، وتكوين مرن، مما يُتيح لموظفي المؤسسات تخزين البيانات ومشاركتها والاحتفاظ بنسخ احتياطية بشكل مركزي عبر خادم موحد[٣].

---

(1) Tantowi L. & Wijayanti L. (2023). PELUANG DAN TANTANGAN PENYIMPANAN CLOUD STORAGE PADA DOKUMEN DIGITAL. Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip Dan Dokumentasi. Vol 15. Is 1. PP 118–131. https://doi.org/10.37108/shaut.v15i1.803.

(2) Mathai M. K. & Mathew J. (2024). Cloud storage. In Research Advances in Network Technologies. 1st Edition. PP 137–154. https://doi.org/10.1201/9781003433958-6.

(3) Ibid. PP 137–154.

يعتمد التخزين السحابي على إدارة ملفات المستندات عبر الإنترنت، مما يتيح الوصول إليها من مواقع مختلفة بشرط توفر اتصال بالإنترنت. تُدار البنية التحتية لهذه الخدمة من قبل مزودي الخدمة، مما يوفر وسيلة تخزين مرنة للأرشيفات الرقمية. قبل انتشار الحوسبة السحابية، كانت هذه الوسائط تُعرف بمحركات الأقراص الافتراضية. يُلغي التخزين السحابي الحاجة إلى وسائط تخزين مادية مثل محركات الأقراص، ويُبسط عملية الإعداد التي تُدار تلقائيًّا من قبل المزود. يتطلب حفظ الملفات اتصالًا بالإنترنت وحسابًا موثقًا لدى مزود الخدمة[١].

تُصنف خدمات التخزين السحابي إلى:-

-التخزين السحابي الشخصي، المستخدم لتخزين البيانات الشخصية مع إمكانية الوصول من أي مكان.

- التخزين السحابي الخاص، المصمم للمؤسسات مع إمكانية الوصول العالمي.

- التخزين السحابي العام، المتاح للجمهور؛ والتخزين السحابي الهجين، الذي يجمع بين الخيارات السابقة. تختلف أنماط استخدام الطلاب للتخزين السحابي بناءً على احتياجاتهم وسلوكياتهم الرقمية، إذ يميلون إلى إدارة الأرشيفات الرقمية عبر مراحل تشمل الاختيار، الترتيب، التجميع، التقييم، وإعادة التجميع، وفقًا لقدراتهم ومعارفهم التقنية. يُظهر هذا التوجه أهمية التخزين السحابي في دعم الأنشطة الأكاديمية وتلبية متطلبات إدارة المعلومات بكفاءة[٢].

(1) M. Harsitha, Lavanya, Manoj Sanikam M. & Mayur Gupta. (2022). A Cloud Storage. International Journal of Advanced Research in Science, Communication and Technology. Vol 2. Is 1. PP 44–52. https://doi.org/10.48175/ijarsct-7064.

(2) Anil Kumar Reddy Avula. (2024). Understanding Cloud Computing: How Data Storage Works in the Cloud. International Journal For Multidisciplinary Research. Vol. 6. Is 6. https://doi.org/10.36948/ijfmr.2024.v06i06.33472.

المطلب الأول
مفهوم التخزين السحابي وأنواعه

في عصر التحول الرقمي، أصبحت البيانات العمود الفقري للمؤسسات والأفراد على حد سواء، إذ تتزايد الحاجة إلى حلول تخزين مرنة، آمنة، وفعالة من حيث التكلفة. يبرز التخزين السحابي بوصفه أحد أهم ابتكارات الحوسبة الحديثة، مقدمًا بديلًا ثوريًّا لوسائط التخزين التقليدية مثل محركات الأقراص الصلبة وأقراص. ويعتمد هذا المفهوم على إدارة البيانات عبر شبكة الإنترنت، مما يتيح الوصول إليها من أي مكان وزمان، ويُعيد تشكيل طريقة تفاعلنا مع المعلومات. وبالتالي؛ لم يعد التخزين مجرد مساحة مادية على جهاز حاسوب أو خادم محلي، بل أصبح خدمة رقمية تحرر الأفراد والمؤسسات من قيود الأجهزة التقليدية، لتمكينهم من الوصول إلى بياناتهم من أي مكان وفي أي وقت[١].

فالتخزين السحابي في أقرب تعريفاته، يُشير إلى نموذج تخزين البيانات الرقمية في مجمعات من الخوادم الافتراضية، بدلًا من حفظها مباشرةً على أجهزة المستخدمين الفردية. هذه الخوادم غالبًا ما تكون مملوكة ومدارة بواسطة مزود خدمة سحابية تابع لجهة خارجية، مثل Google Drive، Dropbox، Microsoft OneDrive، أو Amazon S3. فكر في الأمر كامتلاكك لصندوق ودائع افتراضي في بنك ضخم، إذ يمكنك إيداع وسحب محتوياتك متى شئت، دون القلق بشأن صيانة الصندوق أو أمنه المادي؛ فالبنك (مزود الخدمة السحابية) يتولى كل ذلك[٢].

كما يعبر عن عملية لحفظ البيانات على خوادم بعيدة تُدار من قبل مزودي خدمات سحابية، بدلًا من تخزينها على الأقراص الصلبة المحلية أو الخوادم الداخلية للمؤسسة. وتُرسل هذه البيانات وتُسترجع عبر الإنترنت، مما يوفّر وصولًا فوريًّا ومرنًا من أي مكان وزمان.

وبالتالي؛ فهو خدمة توفير مساحات افتراضية لحفظ ومعالجة البيانات والملفات الرقمية، يُقدمها طرف ثالث (مُزود الخدمة السحابية) عبر شبكة الإنترنت، بحيث تكون هذه البيانات متاحة للمستخدم (العميل) عند الطلب ومن أي مكان أو جهاز، وذلك دون أن يكون لدى المستخدم

---

(1) Eswari R., Vamshi A., & Sultan M. S. (2023). An Efficient Data Storage Technique for User Files in Cloud. In 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS). IEEE. PP 1–6. https://doi.org/10.1109/iq-cchess56596.2023.10391609.

(2) 王哈琴. (2023). 云存储结构模型及云存储架构的比较研究. 内蒙古民族大学学报（自然科学）. Vol 2013. Is 6. PP 642-645. DOI: 10.3969/j.issn.1671-0185.2013.06.008.

معرفة دقيقة بالموقع الفعلي أو البنية التحتية المادية التي تُخزّن عليها بياناته، ويتم هذا بموجب عقد خدمة يحدد حقوق والتزامات الطرفين[١].

وقد تطوّر هذا النموذج استنادًا إلى مبدأ الحوسبة السحابية، الذي يقوم على إتاحة الموارد الحاسوبية بوصفها خدمة، وليست منتجا، ما يتيح للمستخدمين دفع مقابل ما يستخدمونه فقط دون الحاجة إلى امتلاك البنية التحتية[٢].

---

(١) العبارة تشير إلى مجموعة من العناصر المهمة في البيئات القانونية، للتعبير عن مفهوم التخزين السحابي وتشمل:

١- **خدمة توفير مساحات افتراضية:** التخزين السحابي ليس امتلاكًا ماديًّا لخوادم أو أقراص تخزين، بل هو حق انتفاع بمساحة تخزين غير مادية يُوفرها المُزود. ولكنه يُركز على الخدمة (Service) المقدمة، مما يضعه ضمن إطار عقود الخدمات أو عقود تقديم الخدمات التقنية، وليس عقود الإيجار المادي أو البيع.

٢- **لحفظ ومعالجة البيانات والملفات الرقمية:** يُحدد محل الخدمة وهو البيانات الرقمية، التي قد تكون نصوصاً، صوراً، فيديوهات، برامج، أو أي معلومات إلكترونية. كما يشمل أيضًا المعالجة (Processing)، فلا يقتصر دور التخزين السحابي على الحفظ فقط، بل يشمل غالباً إمكانيات الوصول، التعديل، المشاركة، والنسخ الاحتياطي للبيانات.

٣- **يُقدمه طرف ثالث (مُزود الخدمة السحابية) عبر شبكة الإنترنت:** يُبرز طبيعة العلاقة التعاقدية بين مُزود الخدمة (Service Provider) والعميل، إذ يكون المُزود هو الطرف الذي يُدير البنية التحتية ويُوفر الخدمة. ويُشير إلى أن وسيلة تقديم الخدمة هي الإنترنت، مما يُثير قضايا الاختصاص القضائي وتنازع القوانين في حال وجود نزاعات، نظراً للطبيعة العابرة للحدود للإنترنت.

٤- **تكون هذه البيانات متاحة للمستخدم عند الطلب ومن أي مكان أو جهاز:** يُسلط الضوء على خاصية الوصول المرن (On-demand Access) والانتشار الجغرافي (Ubiquity)، وهي من السمات الأساسية للحوسبة السحابية بشكل عام. هذا الجانب له تداعيات على مسائل الأمن السيبراني وحماية البيانات.

٥- **دون أن يكون لدى المستخدم معرفة دقيقة بالموقع الفعلي أو البنية التحتية المادية:** يُشير إلى خاصية تجريد البنية التحتية (Infrastructure Abstraction)، فلا يهتم المستخدم بالتفاصيل التقنية لمكان تخزين بياناته (كخادم معين أو دولة محددة). هذه النقطة تمُثل تحديًا قانونيًّا كبيرًا فيما يتعلق بتطبيق قوانين حماية البيانات والخصوصية، خاصة عند نقل البيانات عبر الحدود.

٦- **بموجب عقد خدمة يحدد حقوق والتزامات الطرفين:** يُؤكد على أن العلاقة بين المُزود والعميل هي علاقة تعاقدية (Contractual). هذا العقد (الذي غالباً ما يكون عقد إذعان يُوافق عليه المستخدم عبر الإنترنت) هو المرجع الأساس لتحديد المسؤوليات، الضمانات، شروط الاستخدام، سياسات الخصوصية، وآليات حل النزاعات

(2) Salunke N. R. (2021). Files Storage & Sharing Platform Using Cloud. International Journal for Research in Applied Science and Engineering Technology. Vol 9. Is 11. PP 1338–1344. https://doi.org/10.22214/ijraset.2021.38994.

وتُشكل هذه الخوادم شبكة متكاملة، يُشار إليها مجازًا بـ "السحابة". عند حفظ البيانات في السحابة، لا تُخزن في مكان واحد فقط، بل تُوزع غالبًا وتُنسخ على خوادم متعددة في مراكز بيانات مختلفة. هذا التوزيع يضمن المرونة العالية (Elasticity)، إذ يمكن للمستخدمين توسيع أو تقليص مساحة التخزين الخاصة بهم حسب الحاجة، دون الحاجة إلى شراء أو تركيب أجهزة جديدة. كما يوفر المتانة (Durability)، فحتى لو تعطل أحد الخوادم، تظل البيانات متاحة لأن نسخًا منها موجودة في أماكن أخرى[١].

كما يستند التخزين السحابي على بنية تقنية متطورة، تعتمد على خوادم افتراضية عملاقة موزعة جغرافيًا في مراكز بيانات حول العالم. يتيح ذلك إمكانية تخزين البيانات بشكل مشترك ومأمون، مع تقليل مخاطر فقدان البيانات الناتجة عن أعطال الأجهزة أو الكوارث الطبيعية. ومن منظور أكاديمي، يمثل هذا النموذج نقلة نوعية في مفهوم الحوسبة وتوزيع الموارد، فقد انتقل التخزين من كونه مكوّنًا ماديًا محدودًا إلى مورد افتراضي غير محدود[٢].

وبالتالي؛ يقترح الباحث تعريفًا للتخزين السحابي على أنه "نموذج حديث لتخزين البيانات يتم من خلاله حفظ المعلومات على خوادم بعيدة مُدارة من قبل مزودي خدمات سحابية، وتكون هذه الخوادم متاحة عبر الإنترنت، مما يُمكّن المستخدمين من الوصول إلى بياناتهم من أي مكان وفي أي وقت، دون الحاجة إلى امتلاك أو صيانة بنية تحتية مادية محلية، ويتم هذا بموجب عقد خدمة يحدد حقوق والتزامات الطرفين".

يعتمد التخزين السحابي على:

١- **مراكز البيانات**: هي منشآت ضخمة تضم آلاف الخوادم، وأنظمة التبريد، ومصادر الطاقة الاحتياطية، وشبكات الاتصال عالية السرعة.

---

(1) Anil Kumar Reddy Avula. (2024). Understanding Cloud Computing: How Data Storage Works in the Cloud. International Journal For Multidisciplinary Research. Op. cit.

(2) Antu A. D., Kumar A., Kelley R. & Xie B. (2022). Comparative Analysis of Cloud Storage Options for Diverse Application Requirements. In Lecture Notes in Computer Science. Springer International Publishing. PP 75–96. https://doi.org/10.1007/978-3-030-96326-2_6.

٢- **الخوادم الافتراضية** (Virtual Servers): بدلًا من تخصيص خادم مادي لكل مستخدم، يتم تقسيم الخوادم المادية إلى وحدات افتراضية يمكن تخصيصها لمستخدمين متعددين، مما يزيد من كفاءة استخدام الموارد.

٣- **شبكات الاتصال** (Networking): شبكات إنترنت قوية وعالية السرعة هي العمود الفقري للتخزين السحابي، لأنها تتيح نقل البيانات بسلاسة بين أجهزة المستخدمين والخوادم السحابية.

٤- **برمجيات الإدارة**: أنظمة معقدة تُدير عملية التخزين، النسخ الاحتياطي، الأمن، والوصول إلى البيانات، وغالبًا ما تكون غير مرئية للمستخدم.

يُقدم التخزين السحابي مجموعة من الفوائد التي جعلته خيارًا مفضلًا للأفراد والشركات على حد سواء[1]:

١- **سهولة الوصول والتعاون**: يُمكّن المستخدمين من الوصول إلى ملفاتهم من أي جهاز متصل بالإنترنت، وفي أي مكان. كما يسهل التعاون على نفس المستندات مع عدة مستخدمين في الوقت الفعلي، مما يعزز الإنتاجية.

٢- **خفض التكاليف**: يُلغي الحاجة إلى شراء وصيانة أجهزة التخزين المادية، مما يقلل من النفقات الرأسمالية والتشغيلية، خاصة للشركات الصغيرة والناشئة. يدفع المستخدمون فقط مقابل المساحة التي يحتاجونها (نموذج الدفع حسب الاستخدام).

٣- **المرونة وقابلية التوسع**: يمكن زيادة أو تقليص مساحة التخزين بسهولة فائقة لتلبية الاحتياجات المتغيرة، دون قيود البنية التحتية المادية.

٤- **الأمان والنسخ الاحتياطي**: يقوم مزودو الخدمة السحابية بتطبيق طبقات متعددة من الأمان المادي والرقمي (مثل التشفير، النسخ الاحتياطي التلقائي، أنظمة كشف الاختراق) التي قد لا تكون متاحة للأفراد أو الشركات الصغيرة، مما يحمي البيانات من الفقدان أو الضياع.

٥- **التوافر الدائم**: بفضل توزيع البيانات على خوادم متعددة، يضمن التخزين السحابي توافر البيانات، حتى في حالة تعطل جزء من النظام.

---

(1) Eswari R., Vamshi A., & Sultan M. S. (2023). An Efficient Data Storage Technique for User Files in Cloud. Op. cit. PP 1–6.

يُمثل التخزين السحابي قفزة نوعية في إدارة البيانات، مقدمًا حلولًا مرنة وفعالة تلبي احتياجات الأفراد والمؤسسات. وعلى الرغم من تحديات الأمان والاتصال، فإن فوائده في تقليل التكاليف، تعزيز التعاون، ودعم الاستدامة تجعله أداة لا غنى عنها. في المنطقة العربية، يمكن للتخزين السحابي أن يدعم طموحات التحول الرقمي، شريطة تعزيز البنية التحتية وزيادة الوعي. كما يُبرز هذا المفهوم قدرة التكنولوجيا على إعادة تشكيل عالمنا، فكما قال بيل غيتس: "المعلومات هي القوة، والتكنولوجيا هي المفتاح لإطلاقها". من خلال الاستثمار في التخزين السحابي، يمكن للمجتمعات العربية أن تُشارك بقوة في بناء مستقبل رقمي مستدام[١].

أنواع التخزين السحابي:

أصبح التخزين السحابي ركيزة أساسية لإدارة البيانات، مقدمًا مرونة غير مسبوقة. ومع ذلك، لا يتخذ التخزين السحابي شكلًا واحدًا، بل يتنوع في نماذجه ليتناسب مع احتياجات المستخدمين المختلفة، سواء كانوا أفرادًا، أو شركات صغيرة، أو مؤسسات عملاقة. ويمكن تصنيف التخزين السحابي بشكل أساس إلى أربعة أنواع رئيسة هي؛ التخزين السحابي الشخصي، الخاص، العام، والهجين. وكل نوع يتميز بخصائصه الفريدة ومجالات تطبيقه[٢]. وفيما يلي تفصل لأنواع التخزين السحابي الأربعة، مع الأمثلة العملية:

١- **التخزين السحابي الشخصي** (Personal Cloud Storage): التخزين السحابي الشخصي هو النمط الأكثر شيوعًا والأسهل في الاستخدام بالنسبة للأفراد. تم تصميم هذا النوع خصيصًا لتلبية احتياجات المستخدمين الفرديين في حفظ، مزامنة، ومشاركة بياناتهم الشخصية عبر أجهزة متعددة[٣].

وهذا النموذج يقوم على تقديم مساحة تخزين على خوادم يديرها مزود خدمة سحابية تابع لجهة خارجية. والمستخدم النهائي لا يملك أو يدير البنية التحتية، بل يستأجر مساحة تخزين ويصل إليها عبر تطبيقات سهلة الاستخدام أو واجهات ويب. والهدف الأساس هو توفير وسيلة مريحة وآمنة

(1) Nordic Public Sector Cloud Computing – a discussion paper. (2012). TemaNord. Nordic Council of Ministers. PP 5-56. https://doi.org/10.6027/tn2011-566.
(2) Marinescu D. C. (2023). Cloud data storage. Cloud Computing Elsevier. PP 215–256. https://doi.org/10.1016/b978-0-32-385277-7.00014-2.
(3) Thi Bao Thu Le, Nicolas Anciaux, Sébastien Gilloton, Saliha Lallali, Philippe Pucheral & et al. (2016). Distributed Secure Search in the Personal Cloud. EDBT - 19th International Conference on Extending Database Technology, Mar 2016. Bordeaux. France. PP 652-655. hal-01293409

لحفظ الملفات بعيدًا عن الأجهزة المحلية، مع ضمان سهولة الوصول إليها من أي مكان وفي أي وقت عبر الإنترنت[١].

يُساعد التخزين السحابي الشخصي الأفراد على الاحتفاظ بنسخة احتياطية دائمة من بياناتهم، وتقليل مخاطر فقدانها في حال تلف الأجهزة أو سرقتها. كما يوفّر إمكانيات مشاركة الملفات بسهولة، ما يعزّز التعاون بين الأفراد.

٢- **التخزين السحابي الخاص** (Private Cloud Storage): التخزين السحابي الخاص نموذجٌ أكثر تعقيدًا وهو مخصص بشكل أساس للمؤسسات الكبيرة أو تلك التي لديها متطلبات صارمة للأمان والخصوصية والتحكم[٢].

وفي هذا النموذج، يتم بناء وتشغيل البنية التحتية للتخزين السحابي وتخصيصها لمؤسسة واحدة فقط. يمكن أن يتم ذلك داخل مركز بيانات المؤسسة نفسه (On-premises private cloud) أو يمكن لمزود خدمة خارجي أن يقوم بإنشاء بنية تحتية مخصصة ومستقلة تمامًا لتلك المؤسسة (Hosted private cloud). الهدف الرئيس هو توفير مزايا السحابة (كالمرونة وقابلية التوسع) مع الحفاظ على أقصى درجات التحكم في البيانات والأمان والامتثال للوائح[٣].

يُحقّق هذا النوع من التخزين السحابي التوازن بين مرونة الحوسبة السحابية والحاجة إلى السيطرة الكاملة على البيانات، ما يجعله خيارًا شائعًا للقطاعات الحساسة.

٣- **التخزين السحابي العام** (Public Cloud Storage): التخزين السحابي العام هو النمط الأكثر شيوعًا وانتشارًا، ويستفيد منه غالبية المستخدمين والأعمال الصغيرة والمتوسطة[٤].

---

(1) Seay C., Washington M. & Watson R. J. (2016). Personal Applications of Clouds. In Encyclopedia of Cloud Computing (Wiley). PP 517–523. https://doi.org/10.1002/9781118821930.ch42.

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

(3) Helmiawan M. A. & Fadil I. (2020). PRIVATE CLOUD STORAGE IN RURAL'S MANAGEMENT AND INFORMATION SYSTEM USING ROADMAP FOR CLOUD COMPUTING ADOPTION (ROCCA). INTERNAL (Information System Journal). Vol 2. Is 2. PP 172–183. https://doi.org/10.32627/internal.v2i2.85.

(4) Vankayalapati R. K. (2025). Public clouds: The pillar of scalability and innovation. The Synergy Between Public and Private Clouds in Hybrid

وفي هذا النموذج، يتم تقديم خدمات التخزين السحابي من قبل مزود خدمة خارجي (طرف ثالث) يمتلك ويدير البنية التحتية بالكامل (الخوادم، الشبكات، مراكز البيانات). يتم مشاركة هذه البنية التحتية بين العديد من العملاء (Multi-tenancy). يدفع المستخدمون عادةً مقابل الاستخدام الفعلي للموارد (Pay-as-you-go) أو وفقًا لخطط اشتراك محددة[١].

٤ـ التخزين السحابي الهجين (Hybrid Cloud Storage): يُقدم التخزين السحابي الهجين حلًّا وسطًا يجمع بين أفضل ما في العالمين: التحكم والأمان للسحابة الخاصة، والمرونة وفعالية التكلفة للسحابة العامة[٢].

يتضمن هذا النموذج دمج بنية تحتية للتخزين السحابي الخاص (محلية أو مستضاف) مع خدمة تخزين سحابي عام. تسمح هذه التركيبة للبيانات والتطبيقات بالانتقال بسلاسة بين البيئتين. الهدف هو تحقيق التوازن الأمثل بين متطلبات الأمان، الامتثال، الأداء، وفعالية التكلفة[٣].

يُسهم هذا النموذج في تعزيز الكفاءة التشغيلية، فيمكن الاحتفاظ بالبيانات الحساسة داخليًّا للامتثال للمعايير التنظيمية، مع الاستفادة من مرونة وقدرة التوسع الكبيرة للتخزين السحابي العام.

Infrastructure Models: Real-World Case Studies and Best Practices. Deep Science Publishing. PP 32-49. https://doi.org/10.70593/978-81-984306-5-6_3.

(1) G. Megala & S. Prabu. (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. Is 5. PP 1273–1280. https://doi.org/10.17762/turcomat.v12i5.1794.

(2) Hongtao Liu. (2024). Optimization and performance improvement of distributed data storage in hybrid storage systems. World Journal of Advanced Engineering Technology and Sciences. Vol 13. Is 1. PP 459–467. https://doi.org/10.30574/wjaets.2024.13.1.0443.

(3) Jiang Y., Li J., Zhang L., Jia Z., Liu W. & Liu C. (2024). Design and Implementation of Secure Cloud Storage System based on Hybrid Cryptographic Algorithm. 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS). IEEE. PP 1–7. https://doi.org/10.1109/iacis61494.2024.10721716.

جدول رقم (١) مقارنة بين الأنواع الأربعة للتخزين السحابي

النوع	المستخدمون	الأمان	التكلفة	المرونة	أمثلة
الشخصي	أفراد	متوسط	منخفضة/ مجانية	عالية	iCloud, Google Drive
الخاص	مؤسسات	عالٍ	مرتفعة	متوسطة	Azure Private Cloud
العام	أفراد/ شركات صغيرة	متوسط	منخفضة	عالية	OneDrive, Amazon S3
الهجين	مؤسسات/ حكومات	عالٍ	متوسطة إلى مرتفعة	عالية	AWS Outposts

الجدول من إعداد الباحث

إن فهم الأنواع المختلفة للتخزين السحابي ضروري لاختيار الحل الأمثل الذي يتناسب مع الاحتياجات المحددة للأفراد أو المؤسسات. مما يُمكّن من الاستفادة القصوى منه مع تحقيق التوازن بين الأداء، الأمان.

المطلب الثاني
خصائص التخزين السحابي

أصبح التخزين السحابي حجر الزاوية في إعادة تشكيل إدارة المعلومات للأفراد والمؤسسات على حد سواء. يعتمد التخزين السحابي على تقنيات الحوسبة السحابية لتخزين البيانات على خوادم بعيدة يمكن الوصول إليها عبر شبكة الإنترنت، مما يُلغي الحاجة إلى وسائط التخزين التقليدية مثل محركات الأقراص الصلبة، ووحدات USB. وتتعدد خصائص التخزين السحابي التي تجمع بين المرونة، الأمان، وقابلية التوسع، مما يجعله أداة حيوية في دعم التحول الرقمي[١]. وفيما يلي تحليل خصائص التخزين السحابي الرئيسة، مع توضيح فوائدها، تحدياتها، وتطبيقاتها العملية في سياقات متنوعة:

١- **قابلية التوسع المرنة** (**Elastic Scalability**): تُعد قابلية التوسع المرنة إحدى أبرز السمات المميزة للتخزين السحابي، التي تمُثله بوصفه تطورا جذريا عن البنى التحتية التقليدية. إذ تُشير قابلية التوسع المرنة إلى قدرة نظام التخزين على زيادة أو تقليل السعة التخزينية وموارد الحوسبة المرتبطة بها (مثل عرض النطاق الترددي وموارد المعالجة) بشكل ديناميكي وتلقائي (On-demand)، استجابةً للتقلبات في حجم البيانات أو متطلبات الأداء. وهذا التحول يتم غالبًا في وقت شبه فوري، دون الحاجة إلى تدخل بشري كبير أو إعادة تهيئة معقدة للبنية التحتية. يعتمد ذلك على تقنيات الافتراضية (Virtualization)، إذ يتم تجريد الموارد المادية (الخوادم، أقراص التخزين) وتحويلها إلى موارد افتراضية يمكن تخصيصها وتقسيمها بمرونة بين العديد من العملاء (Multi-tenancy)[٢].

وتُترجم هذه الخاصية إلى كفاءة اقتصادية فائقة. فبدلًا من الاستثمار الرأسمالي الضخم في شراء وتوفير سعة تخزينية إضافية (Over-provisioning) لمواجهة أقصى حالات الذروة المتوقعة (مما يؤدي إلى موارد غير مستخدمة في الأوقات العادية)، ويُمكّن التخزين السحابي المؤسسات من[٣]:

- **تحسين استخدام الموارد**: الدفع مقابل الموارد المستهلكة فقط، وتجنب الإنفاق على سعة تخزينية غير مستغلة.

---

(1) Dritsas E. & Trigka M. (2025). A Survey on the Applications of Cloud Computing in the Industrial Internet of Things. Big Data and Cognitive Computing. Vol 9. Is 2. PP 44. https://doi.org/10.3390/bdcc9020044.

(2) Mathai M. K. & Mathew J. (2024). Cloud storage. Research Advances in Network Technologies. Op. cit. PP 137–154.

(3) Tantowi L. & Wijayanti L. (2023). PELUANG DAN TANTANGAN PENYIMPANAN CLOUD STORAGE PADA DOKUMEN DIGITAL. Op. cit. PP 118–131.

-**الاستجابة لتقلبات الأعمال**: تلبية الاحتياجات الموسمية أو الطارئة (مثل الحملات التسويقية، أو نمو المستخدمين المفاجئ) بكفاءة، دون القلق بشأن قيود البنية التحتية.

-**تقليل النفقات الرأسمالية** (CAPEX): تحويل التكاليف من استثمارات رأسمالية كبيرة إلى نفقات تشغيلية متغيرة (OPEX).

فإذا كانت هناك شركة ناشئة لتطوير تطبيقات الهاتف المحمول تشهد نموًّا سريعًا في عدد مستخدميها. وكل مستخدم جديد يُنتج بيانات تتطلب تخزينًا. بدلًا من شراء خوادم تخزين جديدة كل بضعة أشهر، تستخدم الشركة خدمة تخزين سحابي تسمح لها بزيادة سعتها التخزينية بلمسة زر واحدة في لوحة التحكم، مما يضمن استمرار تقديم الخدمة دون انقطاع ويحافظ على تركيز الشركة على تطوير المنتج بدلًا من إدارة البنية التحتية[١].

٢- **الدفع حسب الاستخدام** (Pay-as-You-Go/Utility Pricing): تُعد خاصية الدفع حسب الاستخدام جوهر النموذج الاقتصادي للسحابة، وتحاكي إلى حد كبير طريقة الدفع مقابل الخدمات الأساسية مثل الكهرباء أو المياه.

يرتبط هذا النموذج ارتباطًا وثيقًا بقابلية التوسع المرنة. فمزود الخدمة السحابية يُقنن استهلاك الموارد (مثل حجم البيانات المخزنة بالجيجابايت، حجم البيانات المنقولة، عدد طلبات الوصول إلى البيانات)، ويكون الدفع بناءً على هذا الاستهلاك الفعلي، عادةً على أساس شهري. يتضمن هذا النموذج أحيانًا مستويات تسعير مختلفة (Tiered Pricing) بناءً على حجم الاستخدام أو مستوى الأداء المطلوب[٢]. وتتمثل الأبعاد الاقتصادية والعملية في[٣]:

-**التحكم في التكاليف**: يسمح هذا النموذج للمؤسسات بتقدير تكاليف التخزين بشكل أكثر دقة بناءً على الاستخدام الفعلي، وتجنب تكاليف الصيانة الدورية للأجهزة والتحديثات.

---

(1) Dritsas E. & Trigka M. (2025). A Survey on the Applications of Cloud Computing in the Industrial Internet of Things. Op. cit. PP 44.

(2) Mollakuqe E., Hamdiu E., Fishekqiu N. S., Jakupi S. & Qarkaxhija J. (2024). Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte. Op. cit.

(3) Madhusudhan Dasari sreeramulu. (2024). Analysis of Cloud Computing and Cloud Storage in Mobile Forensics Using the DEMATEL Method. Computer Science, Engineering and Technology. Vol 2. Is 2. PP 33–43. https://doi.org/10.46632/cset/2/2/4.

-**مرونة الميزانية**: يمكن للميزانيات المرتبطة بالتخزين أن تتغير صعودًا وهبوطًا مع متطلبات العمل، مما يوفر مرونة مالية كبيرة.

-**خفض الحواجز أمام الدخول**: يُمكّن الشركات الصغيرة والمتوسطة، والشركات الناشئة، من الوصول إلى بنية تحتية متقدمة لا يمكنهم تحمل تكلفتها لو اضطروا لشرائها وتأمينها محليًّا. هذا يعزز الابتكار وريادة الأعمال.

ومثال لتوضيح ذلك؛ إذا أراد مصور فوتوغرافي محترف أن يستخدم التخزين السحابي لحفظ مشاريعه، خلال موسم الذروة، التي يرتفع حجم الملفات المخزنة لديه بشكل كبير في تلك الفترة، وتزيد تكلفة التخزين لديه مؤقتًا. وفي الفترات الأقل نشاطًا، ينخفض حجم البيانات التي يرفعها، وبالتالي تنخفض تكلفة التخزين، مما يضمن له المرونة المالية دون الحاجة للاستثمار في أقراص تخزين صلبة تظل فارغة معظم الوقت.

٣- **التوفر العالي والموثوقية** (High Availability & Reliability): تُعد حماية البيانات من الفقدان والضمان المستمر للوصول إليها من الخصائص المحورية التي تُميز التخزين السحابي عن الحلول المحلية.

فالتوفر العالي يُقصد به قدرة النظام على البقاء تحت التشغيل، ومتاحًا للمستخدمين بشكل مستمر، حتى في مواجهة حالات الفشل الجزئية (مثل تعطل خادم فردي أو شبكة معينة)[١]. يتم تحقيق ذلك من خلال[٢]:

-**التكرار**: تخزين نسخ متعددة من البيانات عبر خوادم مختلفة (Within a data center) و/ أو عبر مناطق توفر متعددة (ضمن منطقة جغرافية واحدة) و/ أو عبر مناطق جغرافية مختلفة تمامًا. هذا يضمن أنه في حال فشل مكون ما، يتم توجيه الطلبات تلقائيًّا إلى نسخة أخرى من البيانات.

---

(1) Antu A.D., Kumar A., Kelley R. & Xie B. (2022). Comparative Analysis of Cloud Storage Options for Diverse Application Requirements. In: Ye K., Zhang LJ. Op.cit. https://doi.org/10.1007/978-3-030-96326-2_6.

(2) Odun-Ayo I., Ajayi O., Akanle B. & Ahuja R. (2017). An Overview of Data Storage in Cloud Computing. 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS). IEEE. PP 29–34. https://doi.org/10.1109/icngcis.2017.9.

-**الموازنة بين الأحمال**: توزيع طلبات الوصول إلى البيانات عبر خوادم متعددة لمنع التحميل الزائد على أي خادم واحد.

والموثوقية تُشير إلى ضمان سلامة البيانات وعدم تعرضها للتلف أو الفقدان. تُحقق من خلال[1]:

-**آليات الكشف عن الأخطاء وتصحيحها** (Error Detection and Correction): استخدام خوارزميات للكشف عن أي تلف في البيانات وتصحيحه تلقائيًا.

-**النسخ الاحتياطي التلقائي** (Automated Backups): تُجرى عمليات نسخ احتياطي منتظمة للبيانات لضمان استعادتها في حال حدوث أي مشكلة كبرى أو حذف غير مقصود.

-**مراقبة البنية التحتية** (Infrastructure Monitoring): مراقبة شاملة ومستمرة للمعدات والبرمجيات لتحديد المشكلات المحتملة قبل أن تؤثر على الخدمات.

وتتمثل الأبعاد الاقتصادية والعملية في[2]:

-**تقليل وقت التوقف عن العمل** (Downtime): تُقلل الموثوقية العالية من فترات انقطاع الخدمة، مما يحمي الإيرادات وسمعة الأعمال التي تعتمد على توافر بياناتها بشكل مستمر.

-**حماية البيانات من الكوارث**: تُوفر آليات التكرار الجغرافي حماية ضد الكوارث الطبيعية أو الحوادث الكبرى التي قد تدمر مركز بيانات كامل.

-**الأمان**: يُمكن للمستخدمين الأفراد والشركات التركيز على أعمالهم الأساسية بدلًا من القلق بشأن صيانة البنية التحتية، وإجراء النسخ الاحتياطية، والتعافي من الكوارث.

ومثال لتوضيح ذلك؛ إذا كانت هناك منصة بث فيديو عالمية تعتمد على التخزين السحابي لتخزين مليارات مقاطع الفيديو الخاصة بها. بفضل التوفر العالي، عندما يحاول ملايين المستخدمين الوصول إلى مقاطع الفيديو في نفس الوقت، يتم توزيع الطلبات عبر آلاف الخوادم. وإذا حدث عطل في أحد مراكز البيانات في قارة ما، يتم توجيه حركة المرور تلقائيًا إلى مركز بيانات آخر في قارة مختلفة يحمل نفس البيانات، مما يضمن استمرارية الخدمة دون انقطاع للمشاهدين.

---

(1) Salunke N. R. (2021). Files Storage & Sharing Platform Using Cloud. International Journal for Research in Applied Science and Engineering Technology. Vol 9. Is 11. PP 1338–1344. https://doi.org/10.22214/ijraset.2021.38994.b.

(2) Anil Kumar Reddy Avula. (2024). Understanding Cloud Computing: How Data Storage Works in the Cloud. International Journal For Multidisciplinary Research. Op. cit.

٤- **الوصول من أي مكان وفي أي وقت** (Anywhere, Anytime Access): لقد حررت هذه الخاصية البيانات من قيود الأجهزة والمواقع الجغرافية. إذ تَعتمد هذه الخاصية على بنية شبكية قوية (شبكة الإنترنت) تمُكن من الوصول إلى البيانات المخزنة على الخوادم السحابية عن بُعد. تُقدم واجهات وصول متعددة، مثل واجهات برمجة التطبيقات (APIs) لتكامل التطبيقات، وواجهات الويب (Web Interfaces) للمستخدمين النهائيين، وتطبيقات الهاتف المحمول. هذا يسمح بالوصول إلى البيانات من أي جهاز متصل بالإنترنت، بغض النظر عن مكانه[١]. وتتمثل الأبعاد الاقتصادية والعملية في[٢]:

-**تعزيز الإنتاجية والتعاون**: يُمكّن فرق العمل الموزعة جغرافيًّا من التعاون على نفس المستندات والملفات في الوقت الفعلي، مما يسرع من وتيرة العمل.

-**مرونة العمل** (Remote Work & Mobile Workforce): يدعم نماذج العمل عن بُعد، إذ يمكن للموظفين الوصول إلى جميع ملفات العمل الضرورية من منازلهم أو أثناء السفر.

-**تيسير المشاركة**: تسهيل مشاركة الملفات والمجلدات مع الزملاء أو الشركاء أو العملاء، مع التحكم في الأذونات.

ولتوضيح ذلك؛ إذا كان هناك فريق تسويق عالمي يعمل على حملة إعلانية جديدة. وأعضاء الفريق في دبي، لندن، ونيويورك يمكنهم جميعًا الوصول إلى نفس المستندات التصميمية، مقاطع الفيديو الترويجية، وجداول البيانات المخزنة في السحابة. يمكنهم إجراء التعديلات، إضافة التعليقات، ومشاركتها في الوقت الفعلي، مما يلغي الحاجة إلى إرسال نسخ متعددة عبر البريد الإلكتروني ويضمن أن الجميع يعمل على أحدث إصدار من الملفات.

٥- **الأمان المتقدم** (Advanced Security): على الرغم من أن نقل البيانات إلى السحابة قد يثير مخاوف أولية بشأن الأمان، فإن مزودي الخدمة السحابية الرائدين يستثمرون بشكل كبير في

---

(1) Marinescu D. C. (2023). Cloud access and cloud interconnection networks. Cloud Computing Elsevier. PP 175–213. https://doi.org/10.1016/b978-0-32-385277-7.00013-0.

(2) Byali R., Jyothi Ms. & Shekadar M. C. (2022). Design and Analysis of Cloud Data's Multi-Layer Security Protection. International Journal of Research Publication and Reviews. Vol 3. Is 8. PP 173–175. https://doi.org/10.55248/gengpi.2022.3.8.5.

توفير مستويات حماية غالبًا ما تتجاوز قدرات المؤسسات الفردية[١]. ويطبق مزودو التخزين السحابي طبقات متعددة ومتطورة من الأمان تشمل[٢]:

- **التشفير** (Encryption): حماية البيانات أثناء انتقالها بين أجهزة المستخدمين والخوادم السحابية (مثال: استخدام بروتوكولات مثل TLS/SSL). وتشفير البيانات في وضع السكون (Encryption at Rest): تشفير البيانات وهي مخزنة على أقراص الخوادم (مثال استخدام AES-256).

- **التحكم في الوصول وإدارة الهوية** (Access Control & Identity Management): المصادقة متعددة العوامل (MFA): تتطلب أكثر من طريقة للتحقق من هوية المستخدم. وإدارة الهوية والوصول (IAM): تحديد دقيق لأذونات المستخدمين على مستوى الملفات والمجلدات وحتى العمليات، مما يضمن أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى بيانات محددة.

-**مراقبة الأمن وكشف التهديدات** (Security Monitoring & Threat Detection): استخدام أنظمة الذكاء الاصطناعي والتعلم الآلي لمراقبة الأنشطة المشبوهة، اكتشاف الاختراقات المحتملة، ورصد أنماط الهجمات السيبرانية.

-**الأمان المادي لمراكز البيانات**: إجراءات أمنية صارمة في مراكز البيانات نفسها، تشمل الأمن البيومتري، المراقبة بالفيديو على مدار الساعة، وأنظمة إطفاء الحريق المتقدمة.

-**الامتثال للمعايير واللوائح** (Compliance): يلتزم مزودو الخدمات السحابية بمعايير أمنية دولية (مثل ISO 27001) ولوائح خصوصية البيانات (مثل GDPR، HIPAA)، مما يساعد العملاء على تحقيق الامتثال الخاص بهم.

---

(1) M. A. Z. Bin Idrus, F. D. A. Rahman, O. O. Khalifa & N. M. Yusoff. (2023). Blockchain-based Security for Cloud Data Storage. 2023 IEEE 9th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Kuala Lumpur, Malaysia. PP 73-77. Doi: 10.1109/ICSIMA59853.2023.10373457.

(2) Mollakuqe E., Hamdiu E., Fishekqiu N. S., Jakupi S. & Qarkaxhija J. (2024). Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte. Open Research Europe. (version 1; peer review: awaiting peer review). 4. 128. https://doi.org/10.12688/openreseurope.16631.1.

وتتمثل الأبعاد الاقتصادية والعملية في[1]:

- **تخفيض تكاليف الأمن**: تتحمل الشركات الصغيرة والمتوسطة تكاليف أمنية أقل بكثير، فيتم تحمل الاستثمار في البنية التحتية الأمنية المتطورة من قبل مزود الخدمة السحابية.
- **خبرة أمنية متخصصة**: يُوظف مزودو السحابة فرقًا من خبراء الأمن السيبراني الذين قد لا تتمكن الشركات الفردية من تحمل تكلفة توظيفهم.
- **حماية أفضل للبيانات**: الاستفادة من أحدث التقنيات والإجراءات الأمنية التي قد لا تكون متاحة للحلول المحلية.

ومثال ذلك؛ إذ كانت هناك مؤسسة مالية تتعامل مع بيانات العملاء الحساسة. وعلى الرغم من أن البيانات مخزنة خارج مبانيها، فإنها تعتمد على مزود خدمة سحابية يُطبق تشفيرًا قويًّا لجميع البيانات، ويُفعل المصادقة متعددة العوامل لجميع الموظفين، ويُراقب الشبكة باستمرار بحثًا عن أي علامات اختراق. هذه الإجراءات تمنح المؤسسة ثقة أكبر في أمان بياناتها، مما يُمكّنها من التركيز على تقديم الخدمات المالية بدلًا من إدارة بنية أمنية معقدة.

تُمثل خصائص التخزين السحابي الخمس الأساسية - قابلية التوسع المرنة، نموذج الدفع حسب الاستخدام، التوفر العالي والموثوقية، الوصول الشامل، والأمان المتقدم - حجر الزاوية في ثورة إدارة البيانات. إنها لا توفر مجرد بديل تقني، بل تُقدم نموذجًا اقتصاديًّا وتشغيليًّا يحول التخزين من مجرد عبء إلى محرك للابتكار، الكفاءة، والمرونة، مما يُمكن الأفراد والمؤسسات من الازدهار في العصر الرقمي المتغير. وبفضل هذه المزايا، أصبح التخزين السحابي حجر الأساس لعصر الأعمال الحديث والاقتصاد الرقمي، مما يدفعنا لاستكشاف المزيد من طرق استثماره لتلبية احتياجات المستقبل.

---

(1) J. B K & T. J. (2022). Data Storage Security and Privacy in Cloud Computing. 2022 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE), Bangalore, India. PP 1-10. doi: 10.1109/ICWITE57052.2022.10176237.

المبحث الثاني
التحديات القانونية المرتبطة بالخدمات السحابية

مع تسارع وتيرة التحول الرقمي، أصبح التخزين السحابي أحد المكونات الأساسية للبنية التحتية للبيئة المعلوماتية الحديثة، إذ تلجأ إليه الشركات والمؤسسات والأفراد لحفظ البيانات واسترجاعها بمرونة وكفاءة عبر الإنترنت، دون الحاجة إلى امتلاك أنظمة تخزين محلية. غير أن هذا التحول لم يأتِ دون تحديات قانونية، إذ أفرز بيئة خصبة لنشوء نزاعات قانونية متشابكة تمس حقوق الأطراف المختلفة، وتثير إشكاليات عميقة تتعلق بالولاية القضائية، وحماية البيانات، والمسؤولية القانونية.

وتنشأ النزاعات القانونية في بيئات التخزين السحابية من تعقيدات الولاية القضائية وخصوصية البيانات والامتثال للقوانين الوطنية المختلفة، والحيازة (ملكية المحتوى السحابي). نظرًا لأن التكنولوجيا السحابية تتجاوز الحدود الجغرافية، فإن الأطر القانونية غالبًا ما تتخلف عن الركب، مما يؤدي إلى النزاعات والشكوك. تشمل القضايا الرئيسة سيادة البيانات والمسؤولية عن فشل الخدمة وتحديات وصول سلطات إنفاذ القانون إلى البيانات المخزنة في السحابة. ويُعزى تعقيد هذه النزاعات إلى الطبيعة غير المادية للتخزين السحابي، واعتماده على بنية موزعة جغرافيًّا، مما يُصعّب تحديد الاختصاص المكاني، ويُعقد تكييف العلاقة القانونية بين الأطراف[١].

تُعرّف النزاعات القانونية في سياق التخزين السحابي بأنها المنازعات التي تنشأ بين الأطراف ذات العلاقة بخدمات الحوسبة السحابية "مثل مزوّدي الخدمة والعملاء والمستخدمين الثانويين" نتيجة الإخلال بشروط الخدمة، أو وقوع أضرار، أو خرق الخصوصية، أو الملكية، أو حتى الجرائم المعلوماتية. وتختلف طبيعة هذه النزاعات، فقد تكون مدنية عندما يتعلق الأمر بالتعويضات أو فسخ العقود، أو تجارية متى ارتبطت بإخلال تعاقدي، أو جنائية إذا تعلقت بتسريب البيانات أو استخدامها في أنشطة غير مشروعة[٢].

---

(1) Karagiannis, C., & Vergidis, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. Information. Vol 12. Is 5. PP 181(1-16). https://doi.org/10.3390/info12050181.

(2) Saini J. S., Saini D. K., Gupta P., Lamba C. S. & Rao G. M. (2022). Cloud Computing: Legal Issues and Provision. Security and Communication Networks. Vol 2022. PP 1–13. https://doi.org/10.1155/2022/2288961.

المطلب الأول
طبيعة النزاعات القانونية في بيئات التخزين السحابي

يمثل التخزين السحابي تطورًا بارزًا في أساليب حفظ ومعالجة البيانات، غير أنه يفتح المجال لنشوء أشكال جديدة من النزاعات القانونية، بسبب الطبيعة التقنية المعقدة، وتعدد الأطراف، وتباين النظم القانونية التي تحكم هذا الفضاء الرقمي[١]. ويمكن تصنيف النزاعات القانونية في هذا السياق إلى الفئات التالية:

١- **نزاعات أمن البيانات والخصوصية**: تُعد قضايا خروقات البيانات من أخطر التحديات القانونية في البيئة السحابية، نظرًا لما تسببه من خسائر مادية جسيمة[٢]، وأضرار فادحة بسمعة الأطراف المتورطة[٣].

إذ تنشأ هذه النزاعات عند حصول الوصول غير المشروع إلى البيانات، أو تسريبها، أو تعديلها دون إذن، أو تدميرها نتيجة ثغرات أمنية أو هجمات سيبرانية. وتُعد هذه الأفعال خرقًا صريحًا

---

(1) Hammer A., Ohlig M., Geus J. & Freiling F. (2023). A Functional Classification of Forensic Access to Storage and its Legal Implications. Digital Threats: Research and Practice. Vol 4. Is 3. PP 1–14. https://doi.org/10.1145/3609231.

(٢) تُعد خروقات البيانات من أخطر التحديات التي تواجه البيئة السحابية، لما تنطوي عليه من مخاطر مباشرة على خصوصية الأفراد وسرية المعلومات المؤسسية. فقد يؤدي مجرد خلل أمني يسير إلى تسريب كميات هائلة من البيانات الحساسة، مما يُعرّض الأطراف المتضررة لخسائر مالية، وتشويه السمعة، ومساءلات قانونية متعددة. ويُعد ما حدث في واقعة اختراق قاعدة بيانات Le Figaro مثالًا بالغ الأهمية، فقد أسفر الهجوم السيبراني عن تسريب ما يقرب من ٧.٤ مليار سجل بيانات، الأمر الذي يُجسّد بوضوح حجم الأضرار المحتملة الناتجة عن خروقات البنية السحابية.

وتبرز في هذا السياق إشكالية تحديد المسؤولية القانونية في حال وقوع مثل هذه الاختراقات: هل تقع على عاتق مزوّد الخدمة السحابية لقصوره في تأمين البنية التحتية؟ أم على المستخدم الذي أهمل تطبيق سياسات الحماية المناسبة؟ إن هذا التداخل في المسؤوليات يُشكّل موضع خلاف متكرر في النزاعات السحابية، ويستدعي وجود معايير قانونية دقيقة تُحدّد نطاق الالتزامات التقنية والتعاقدية بين الأطراف، لضمان الحماية القانونية الفاعلة وتقليل الآثار السلبية لمثل هذه الحوادث.

(3) Pimenta Rodrigues G. A., Marques Serrano A. L., Lopes Espiñeira Lemos A. N., Canedo E. D., Mendonça F. L. L. d., de Oliveira Albuquerque R., Sandoval Orozco A. L. & García Villalba L. J. (2024). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. Data. Vol 9. Is 2. PP 27. https://doi.org/10.3390/data9020027.

لالتزامات السرية وحماية البيانات المنصوص عليها في القوانين الوطنية والدولية، مثل اللائحة العامة لحماية البيانات (GDPR) أو قانون خصوصية المستهلك في كاليفورنيا (CCPA)[١].

ويدور النزاع غالبًا حول تحديد المسؤولية القانونية بين مزوّد الخدمة والعميل. ففي حين يُفترض أن يلتزم المزوّد بتوفير بنية أمنية قوية، قد يدفع بأنه غير مسؤول عن الإعدادات التي يجُريها المستخدم (misconfigurations). وهنا تُطرح أسئلة عن معايير الإهمال، ومتى يُعد المزوّد مقصرًا في حماية البيانات[٢].

فإذا تم اختراق قاعدة بيانات لعملاء شركة تخزين إلكتروني بسبب ثغرة في الخادم، قد تُقاضي الشركة المزود لخرق التزامه التعاقدي، في حين قد يدّعي الأخير أن المستخدم هو من فشل في تفعيل جدران الحماية أو إعداد التشفير.

٢ـ **نزاعات الملكية الفكرية**: تُثير خدمات التخزين السحابي إشكالات قانونية متعلقة بحماية حقوق الملكية الفكرية للمحتوى الرقمي المخزن والمُتداول عبر السحابة. إذ تبرز هذه النزاعات عند تحميل أو تداول أو استخدام محتوى محمي بحقوق التأليف أو العلامات التجارية أو الأسرار التجارية دون ترخيص أو تفويض. ويكتسب النزاع بعدًا خاصًّا إذا أتاح المزوّد هذا المحتوى لمستخدمين آخرين دون فحص مشروعية محتواه[٣].

وهنا يُطرح التساؤل حول مدى التزام مزوّد الخدمة بمراقبة المحتوى الذي يحُمّله المستخدمون، وهل هو مسؤول قانونيًّا عن المحتوى غير المشروع إذا تم الإبلاغ عنه ولم يُزله. ويُناقش هنا مبدأ

---

(1) Alugoju N. R. (2024). Data Protection in the Cloud: Ensuring Security and Compliance for Organizational Data. International Journal for Research in Applied Science and Engineering Technology. Vol 12. Is 12. PP 1590–1596. https://doi.org/10.22214/ijraset.2024.66087.

(2) F. Spanca & A. Salihu. (2024). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE). Kuala Lumpur, Malaysia. PP 1-8. doi: 10.1109/ICECCE63537.2024.10823432.

(3) X. Zuo & H. Ding. (2020). Research on Digital Copyright Infringement Based on Cloud Computing Environment. 2020 International Conference on Computer Engineering and Application (ICCEA). Guangzhou, China. PP 128-133, doi: 10.1109/ICCEA50009.2020.00034.

"الدور الوسيط" (intermediary liability) المنصوص عليه في قوانين مثل " Digital Millennium Copyright Act" الأمريكي[١].

فإذا قام أحد موظفي شركة تصميم برفع ملفات تتضمن صورًا مرخّصة للاستخدام الشخصي فقط إلى حساب الشركة السحابي، واستُخدمت هذه الصور في حملات تجارية، قد يُقاضي صاحب الحقوق الشركة ويُحمّلها مسؤولية الاستخدام غير المشروع، مع احتمال إدخال مزوّد الخدمة طرفًا في الدعوى لعدم حجب أو إزالة المحتوى المخالف.

٣- **نزاعات عقود الخدمة (SLAs) والمسؤولية التعاقدية**: تمثل اتفاقيات مستوى الخدمة (SLAs) الإطار القانوني الأساس الذي يُنظّم العلاقة بين مزوّد الخدمة السحابية والمستخدم. فتنشأ النزاعات عند إخلال المزوّد بالتزامات الأداء المتفق عليها مثل مدة التوافر (Uptime)، جودة الاتصال، أو سرعة استعادة البيانات. وغالبًا ما تحتوي العقود على بنود تقيد المسؤولية أو تُحدد سقفًا للتعويضات، وهو ما يكون محل جدل قانوني[٢].

كما تتعلق الإشكالية الأساسية بـ توازن القوة العقدية، إذ عادة ما تُعد عقود SLAs من طرف واحد، وتُفرض على المستخدم دون تفاوض، ما قد يُنتج شروطًا مجحفة أو غير متناسبة. فإذا تعرضت شركة تعتمد على التخزين السحابي لانقطاع في الخدمة استمر لأيام، متجاوزًا النسبة المنصوص عليها في العقد، قد تطالب بتعويضات عن الخسائر، إلا أن المزود قد يستند إلى بند تقنين التعويض (Liquidated Damages)، ما يُعقد المطالبة القضائية[٣].

٤- **نزاعات السيادة على البيانات والوصول الحكومي**: تُعد هذه النزاعات من أكثر القضايا تعقيدًا لما تنطوي عليه من أبعاد سيادية وتشريعية عابرة للحدود. فتنشأ نزاعات سيادة البيانات من

---

(1) Vaibhav Kharose, Himanshu Mevada, Yash Ambarle, Tushar Devre & Shatabdi Bhalerao. (2024). A Cloud-based Multimedia Storage Protection System. International Journal For Multidisciplinary Research. Vol 6. Is 2. https://doi.org/10.36948/ijfmr.2024.v06i02.19320.

(2) Rane D., Chourey V., Verma R. & Gupta P. (2022). Consideration of Availability and Reliability in Cloud Computing. In Machine Learning and Optimization Models for Optimization in Cloud. Chapman and Hall/CRC. PP 55–72. https://doi.org/10.1201/9781003185376-4.

(3) Qazi F., Kwak D., Khan F. G., Ali F., & Khan S. U. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges. Internet of Things. Vol 25. P e101126. https://doi.org/10.1016/j.iot.2024.101126.

تعقيدات حوكمة الإنترنت العالمية، لا سيما فيما يتعلق بوصول الحكومة إلى البيانات المخزنة عبر الحدود. وفي الوقت الذي تتصارع فيه الدول مع الآثار المترتبة على القوانين التي تتجاوز الحدود الإقليمية، يصبح التوازن بين السيادة الوطنية والتعاون الدولي مثيرًا للجدل بشكل متزايد[١].

وعندما تطالب جهة حكومية بالوصول إلى بيانات معينة موجودة في خوادم شركة سحابية تقع خارج أراضيها، بناءً على قوانين وطنية مثل "قانون السحابة الأمريكي (CLOUD Act)"، فيتعارض هذا الطلب مع قوانين حماية البيانات في بلد آخر. ويكون مزوّد الخدمة في موقف حرج: بين الامتثال لأمر قضائي من دولة ما، واحترام قوانين الخصوصية لدولة أخرى. وقد يترتب على الامتثال مسؤولية مدنية أو جزائية في الدولة الأخرى[٢].

فإذا طلبت السلطات الأمريكية من مزوّد سحابي أمريكي تسليم بيانات تخص مواطنين أوروبيين مخزنة على خوادم في أيرلندا، فإن ذلك قد يشكل خرقًا لقوانين حماية البيانات الأوروبية (GDPR)، ويعرض المزود لمساءلة قانونية متعددة الأطراف.

٥- **النزاعات ذات البعد الجنائي**: تمتد النزاعات القانونية إلى المجال الجنائي عندما يتم استغلال بيئات التخزين السحابي في أنشطة غير مشروعة، مثل تخزين أو توزيع محتوى غير قانوني (مواد مقرصنة، محتوى ضار، برمجيات خبيثة). فالنزاعات القانونية في المجال الجنائي فيها تعقيد بسبب استغلال بيئات التخزين السحابية للأنشطة غير القانونية. نظرًا لأن مجرمي الإنترنت يستخدمون هذه المنصات لتخزين وتبادل المواد غير المشروعة، يواجه تطبيق القانون تحديات كبيرة في جمع الأدلة الرقمية وتقديمها. تسهم تعقيدات الولاية القضائية وملكية البيانات وطبيعة

(1) Gao H. (2023). Data Sovereignty and Trade Agreements. In Data Sovereignty. Oxford University Press, New York. PP 213–239. https://doi.org/10.1093/oso/9780197582794.003.0010.

(2) N. Kushwaha, P. Roguski and B. W. Watson. (2020). Up in the Air: Ensuring Government Data Sovereignty in the Cloud. 2020 12th International Conference on Cyber Conflict (CyCon). Estonia. PP 43-61. doi: 10.23919/CyCon49761.2020.9131718.

التكنولوجيا السحابية في هذه النزاعات القانونية. فهل يتحمل مزوّد الخدمة المسؤولية الجنائية لعدم قيامه بالمراقبة الكافية؟ وهل يمكن مساءلته بوصفه فاعلا أصليا أم مجرد وسيط[١]؟

كقيام أحد المستخدمين بتخزين محتوى مقرصن على منصة سحابية بهدف توزيعه لاحقًا، يفتح المجال أمام ملاحقته جنائيًّا، وربما مساءلة المزود إذا تبيّن علمه أو تقصيره في الإزالة[٢].

٦- **نزاعات الاختصاص القضائي**: تشكل مسألة الاختصاص واحدة من أعقد الإشكالات في البيئة السحابية، إذ لا تتحدد مكانة البيانات بحدود جغرافية واضحة. فتنشأ النزاعات حين تختلف الدول في تحديد المحكمة المختصة أو القانون الواجب التطبيق. ويرتبط هذا الخلاف غالبًا بـ "موقع الخادم"، و"جنسية الأطراف"، و"مكان وقوع الضرر"[٣].

ففي قضية Microsoft الشهيرة (٢٠١٣–٢٠١٨)، التي رفضت فيها الشركة تسليم بيانات مخزنة في أيرلندا بناءً على أمر قضائي أمريكي، قبل أن يصـــدر قانون CLOUD Act لتجـــاوز هذه الإشكالية[٤]،

(1) Karagiannis C. & Vergidis K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. Op.cit. PP 181(1-16).
(2) R. S. Sree & K. Raja. (2022). A Review on Forensic Investigation Analysis in Cloud Computing Environments," 2022 1st International Conference on Computational Science and Technology (ICCST). CHENNAI, India. PP 1067-1074. doi: 10.1109/ICCST55948.2022.10040384.
(3) Berman P. S. (2018). Legal Jurisdiction and the Deterritorialization of Data. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3134782.

(٤) هذه القضية، المعروفة باسم Microsoft Ireland Case، كانت نقطة تحول في الجدل حول سيادة البيانات والحدود القانونية للولايات المتحدة فيما يتعلق بالوصول إلى المعلومات المخزنة خارج أراضيها.

في ديسمبر ٢٠١٣، أصدر قاضٍ في المنطقة الجنوبية لنيويورك أمرًا قضائيًّا يطالب مايكروسوفت بتقديم بيانات مستخدم مخزنة في مركز بياناتها في دبلن، أيرلندا، بوصفها جزءا من تحقيق جنائي أمريكي. مايكروسوفت رفضت الامتثال لهذا الأمر، بحجة أن البيانات المخزنة خارج الولايات المتحدة لا تخضع للولاية القضائية الأمريكية بموجب قانون الاتصالات المخزنة (Stored Communications Act - SCA) لعام ١٩٨٦.

بعد معركة قانونية طويلة، قضت محكمة الاستئناف للدائرة الثانية في يوليو ٢٠١٦ بأن الحكومة الأمريكية لا يمكنها إجبار مايكروسوفت أو أي شركة أخرى على تسليم بيانات مخزنة خارج الولايات المتحدة باستخدام أمر قضائي صادر بموجب SCA. ومع ذلك، في عام ٢٠١٨، أقر الكونغرس الأمريكي قانون السحابة (CLOUD Act)، الذي منح السلطات الأمريكية صلاحيات أوسع للوصول إلى البيانات المخزنة دوليًّا، مما أدى إلى إنهاء القضية عمليًّا.

مما يعكس النزاع الصريح بين الأنظمة القضائية في البيئة العابرة للحدود[1].

يتضح أن النزاعات القانونية في بيئة التخزين السحابي لا تنحصر في إطار تقني أو عقدي، بل تمتد إلى الفضاء السيادي والجنائي والدولي، بما يعكس الحاجة إلى تطوير إطار قانوني مرن ومتكامل يُراعي الطبيعة الموزعة لهذا الفضاء الرقمي، ويوازن بين الحقوق الفردية، والمصالح الاقتصادية، ومتطلبات الأمن القومي للدول.

(1) Nora Ellingsen. (2016). The Microsoft Ireland Case: A Brief Summary. The Lawfare Institute. Available through the following link: https://tinyurl.com/27deccsp. It was viewed on: 13/5/2025.

المطلب الثاني
تحليل للمنهج القانوني المرتبط بالخدمات السحابية

لقد أحدثت الخدمات السحابية ثورة في نموذج تقديم واستهلاك الموارد الحاسوبية، محوّلةً البنية التحتية التقليدية إلى نموذج مرن و"افتراضي". ومع أن هذه الثورة جلبت معها كفاءة غير مسبوقة وابتكارًا متسارعًا، إلا أن طبيعتها اللامركزية، وكونها عابرة للحدود، والمبهمة في كثير من الأحيان، قد خلقت حزمة من التحديات القانونية المعقدة. هذه التحديات ليست مجرد عقبات بيروقراطية، بل هي قضايا جوهرية تتعلق بالسيادة الوطنية، وحماية الحقوق الفردية، وتوزيع المسؤوليات، مما يستدعي تدقيقًا قانونيًّا عميقًا[١].

١ـ الولاية القضائية وتضارب القوانين (Jurisdiction and Conflict of Laws):

ربما يكون هذا التحدي هو الأبرز والأكثر تعقيدًا في البيئة السحابية. إن غياب الحدود المادية للبيانات في السحابة يُعقد تحديد القانون الواجب التطبيق والجهة القضائية المختصة. فتُخزن البيانات في السحابة على خوادم قد تتوزع جغرافيًّا عبر دول مختلفة. في حالة نشوء نزاع، أو طلب من جهة حكومية للوصول إلى البيانات[٢]، يبرز السؤال: أي قانون دولة يجب أن يُطبق؟ هل هو قانون البلد الذي ينتمي إليه صاحب البيانات، أم قانون البلد الذي يقع فيه مركز البيانات، أم قانون بلد مزود الخدمة الرئيس[٣]؟

كما تختلف القوانين المتعلقة بحماية البيانات والخصوصية بشكل كبير بين الدول. على سبيل المثال، قد يفرض الاتحاد الأوروبي قيودًا صارمة على نقل البيانات الشخصية خارج أراضيه (مثل اللائحة العامة لحماية البيانات – GDPR)، بينما قد تُجبر قوانين أخرى (مثل قانون CLOUD Act الأمريكي) مزود الخدمة على تسليم بيانات، حتى لو كانت هذه البيانات تخص مواطنين من

---

(1) Krishnan S. & Chen L. (2019). Legal Concerns and Challenges in Cloud Computing. (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1905.10868.

(٢) ومثال على ذلك؛ إذا كانت هناك شركة مصرية تستخدم خدمة تخزين سحابي مقرها الرئيس في الولايات المتحدة، ولها مراكز بيانات موزعة في أيرلندا وألمانيا. إذا طلبت جهة قضائية مصرية (بموجب قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠) بيانات معينة لعميل مصري، فإن مزود الخدمة الأمريكي قد يجد نفسه في مواجهة قوانين أمريكية، أوروبية، ومصرية، كل منها بمتطلبات وإجراءات مختلفة، وقد تُفرض عليه عقوبات في حال عدم امتثاله لأي منها.

(3) Zhang Y. (2023). Legal Approach to International Cooperation on Cloud Storage of Personal Information. Technium Social Sciences Journal. Vol 40. Is 1. PP 156–165. https://doi.org/10.47577/tssj.v40i1.8341.

دول أخرى ومخزنة خارج الولايات المتحدة. هذا التضارب يضع مزودي الخدمات السحابية في موقف لا يُحسدون عليه بين الالتزام بقوانين متعددة ومتعارضة[١].

٢ـ **حماية البيانات والخصوصية** (Data Protection and Privacy): تُعد حماية البيانات الشخصية وحقوق الخصوصية من أبرز أولويات التشريعات الحديثة، وتُشكل تحديًا جوهريًّا في نموذج السحابة. فعند استخدام الخدمات السحابية، يفقد العميل (مالك البيانات) جزءًا من التحكم المباشر ببياناته، إذ تنتقل هذه السيطرة إلى مزود الخدمة السحابية. هذا يُثير تساؤلات حول مدى قدرة العميل على فرض سياسات الخصوصية الخاصة به وضمان التزام المزود بها[٢].

وتُعد هذه النقطة محورية، خاصة مع تزايد عدد الدول التي تُصدر قوانين لحماية البيانات الشخصية. فكثير من هذه القوانين (مثل GDPR الأوروبي، وقانون حماية البيانات الشخصية المصري) تفرض قيودًا صارمة على نقل البيانات الشخصية إلى دول أخرى لا تُقدم مستوى كافيًا من الحماية. هذا يتطلب آليات قانونية معقدة (مثل البنود التعاقدية القياسية – SCCs) لضمان مشروعية النقل[٣].

ففي حال حدوث اختراق أمني يؤدي إلى تسريب بيانات، يبرز التحدي في تحديد المسؤولية القانونية. هل هي مسؤولية مزود الخدمة الذي يجب أن يوفر أمانًا كافيًا؟ أم مسؤولية العميل الذي قد يكون قد أخطأ في تكوين إعدادات الأمان أو لم يُطبق سياسات داخلية صارمة؟ غالبًا ما تُلقي عقود الخدمات السحابية بعبء كبير من المسؤولية على العميل فيما يُعرف بـ "نموذج المسؤولية المشتركة[٤]".

---

(1) Saini J. S., Saini D. K., Gupta P., Lamba C. S. & Rao G. M. (2022). Cloud Computing: Legal Issues and Provision. Op. cit. Vol 2022. PP 1–13.

(2) Kun E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Computer Law & Security Review. Vol 52. P e105931. https://doi.org/10.1016/j.clsr.2023.105931.

(3) Y. Zheng, X. Lu, J. Zhai and Y. Zhu. (2023). Reflections on Digital Legislative Management of Privacy under the background of Cloud Service. 2023 International Conference on Intelligent Management and Software Engineering (IMSE). Rome, Italy. PP 100-103, doi: 10.1109/IMSE61332.2023.00027.

(4) Kaile Sun. (2024). Challenges and Solutions in Cloud Computing Security and Privacy Protection. Journal of Electronics and Information Science. Vol. 9. Is 1. PP 62-68. http://dx.doi.org/10.23977/10.23977/jeis.2024.090110.

فالالتزام بقانون حماية البيانات الشخصية المصري، الذي يتطلب من المؤسسات المصرية التي تستخدم الخدمات السحابية الالتزام بعدة مبادئ، منها الحصول على الموافقة الصريحة لجمع ومعالجة البيانات، وتأمين البيانات، والإخطار في حال حدوث خروقات. هذا يضع مسؤولية كبيرة على العميل للتأكد من أن مزود الخدمة السحابية يمكنه مساعدته في الامتثال لهذه المتطلبات[١].

٣- الملكية الفكرية (Intellectual Property - IP): تُثير بيئة التخزين السحابي تحديات جديدة فيما يتعلق بحقوق الملكية الفكرية، سواء للمحتوى المخزن أو للتقنيات المستخدمة. وبينما تنص معظم عقود الخدمات السحابية على أن العميل يحتفظ بملكية بياناته، إلا أن بعض العقود قد تتضمن بنودًا غامضة تمنح المزود حقوق استخدام واسعة للمحتوى (مثل تحليل البيانات لتحسين الخدمات)، مما قد يتعارض مع حقوق الملكية الفكرية للعميل[٢].

فعندما يقوم مستخدم بتحميل محتوى محمي بحقوق الطبع والنشر بشكل غير قانوني إلى السحابة، يُطرح سؤال حول مسؤولية مزود الخدمة السحابية. هل هو مجرد "ناقل" (Conduit) للمحتوى، أم "مُضيف" (Host) يجب عليه اتخاذ إجراءات لإزالة المحتوى المخالف فور علمه به؟

إذ تعتمد العديد من الشركات على برمجيات وتطبيقات (SaaS) يُقدمها مزود الخدمة السحابية. هذا يُثير تساؤلات حول تراخيص هذه البرمجيات، وحقوق العميل في الوصول إلى الكود المصدري أو نقل التطبيق في حال الرغبة في تغيير المزود[٣].

٤-المسؤولية التعاقدية وتحديد الالتزامات (Contractual Liability and Obligation Definition): تُعد عقود مستوى الخدمة (SLAs) حجر الزاوية في العلاقة بين العميل ومزود الخدمة السحابية، ولكنها غالبًا ما تكون مصدرًا للنزاعات. وتُدرج معظم عقود

---

(1) Chawki M. (2024). An effective cloud computing model enhancing privacy in cloud computing. Information Security Journal: A Global Perspective. Vol 33. Is 6. PP 635–658. https://doi.org/10.1080/19393555.2024.2307637.

(2) Zuo X. & Ding H. (2020). Research on Digital Copyright Infringement Based on Cloud Computing Environment. Journal of Physics: Conference Series. Vol 1607. Is 1. P e012078. https://doi.org/10.1088/1742-6596/1607/1/012078.

(3) 杨健, 王剑 & 杨邓奇. (2014). 版权与数字内容分离的云存储 DR M 方案. 计算机工程与设计. 年卷 35. 期 7. PP 2330-2334. DOI: 10.3969/j.issn.1000-7024.2014.07.014.

الخدمات السحابية بنودًا تحُدد مسؤولية المزود بشكل كبير في حالة الفشل أو الضرر، وقد تُقلل التعويضات المستحقة للعميل إلى مبالغ رمزية لا تُغطي الخسائر الفعلية. هذا يضع عبئًا كبيرًا على العميل في تقدير المخاطر[١].

وفي بعض الأحيان، تحُدد العقود تعويضات محددة سلفًا في حال خرق SLA (مثل خصم نسبة مئوية من الفاتورة). لكن هذه التعويضات قد لا تكون كافية لتغطية التكاليف الحقيقية لوقت التوقف عن العمل أو فقدان البيانات. كما يمكن الحد من المسؤولية التعاقدية من خلال بنود تحدد الحد الأقصى للعقوبات أو الشروط كالقوة القاهرة. ومع ذلك، لا يمكن استبعاد المسؤولية عن الخرق المتعمد، ولا يُسمح بالقيود في العقود التي تشمل المستهلكين أو حيث تنطبق اللوائح القانونية[٢].

ففي بيئات السحابة المعقدة، قد يتعامل العميل مع عدة مزودين لخدمات مختلفة (مثلًا، مزود للبنية التحتية، وآخر للتطبيق، وثالث للأمن). هذا التشعب يُصعب تحديد من المسؤول عن أي خلل أو ضرر يلحق بالخدمة أو البيانات. وغالبًا ما تُقدم عقود الخدمات السحابية كعقود "الإذعان"، إذ يكون المزود هو الطرف القوي الذي يفرض شروطه، ويُصبح التفاوض على بنودها أمرًا صعبًا[٣].

٥- الامتثال التنظيمي والتشريعات الخاصة (Regulatory Compliance and Sector-Specific Regulations): تُجبر المؤسسات على الامتثال لمجموعة كبيرة من القوانين واللوائح، التي يجب أن تمتد إلى استخدامها للخدمات السحابية. فالعديد من الصناعات (مثل المالية، الرعاية الصحية) تفرض متطلبات صارمة للاحتفاظ بأنواع معينة من البيانات لفترات زمنية محددة ولأغراض التدقيق. يجب على المؤسسات التأكد من أن مزود الخدمة السحابية يمكنه تلبية هذه المتطلبات[٤].

---

(1) Pichonnaz P. (2024). Contractual Limitations of Liability and their Impact on Tort Claims. Journal of European Tort Law. Vol 15. Is 1. PP 44-62. https://doi.org/10.1515/jetl-2024-0004.

(2) Mayorova L. A. (2022). Liability clauses in civil law. Siberian Law Herald. Vol 2022. Is 2. PP 75–79. https://doi.org/10.26516/2071-8136.2022.2.75.

(3) Tabatadze T. (2023). The relation of the principle of good faith to the limiting and excluding circumstances of contractual liability. Journal of Contemporary Law. Vol 2. Is 2. PP 170–179. https://doi.org/10.31578/jcl.v2i2.30.

(4) Dharga Panduranga Kolla. (2024). Automating Real-Time Compliance Data Collection in Cloud Architectures: A Technical Deep Dive. International Journal For Multidisciplinary Research. Vol 6. Is 6. https://doi.org/10.36948/ijfmr.2024.v06i06.33599.

إذ نجد أنه قد تتطلب اللوائح قدرة المؤسسة على إجراء عمليات تدقيق ومراجعة لكيفية إدارة بياناتها في السحابة، وهو ما يتطلب شفافية وتوفير سجلات دقيقة من جانب المزود. ففي قطاعات مثل المحاماة أو الطب، تُفرض التزامات صارمة بالسرية. استخدام السحابة يتطلب ضمانات قانونية وتقنية للحفاظ على هذه السرية[١]. كما تفرض هذه القوانين متطلبات محددة على البنوك والمؤسسات المالية فيما يتعلق بتخزين ومعالجة بيانات العملاء، وقد تُقيد استخدام السحابة خارج الحدود الوطنية أو تفرض ضوابط صارمة على المزودين[٢].

٦- **إشكالية ملكية البيانات والسيطرة عليها**: تُثير البيئة السحابية كذلك إشكالية قانونية دقيقة تتعلق بـ تحديد الجهة المالكة للبيانات المخزنة، والتمييز بين "الملكية الفعلية" و"السيطرة التقنية" عليها. فعلى الرغم من أن العميل هو من يُنشئ البيانات أو يملك الحق في استخدامها، فإن الخوادم التي تحتويها تقع تحت سيطرة مزوّد الخدمة، الذي قد يُقيّد الوصول إليها أو يتحكم في معالجتها[٣].

وتُصبح هذه الإشكالية أكثر حدة في حال انتهاء العلاقة التعاقدية بين الطرفين، أو حدوث نزاع حول استرداد البيانات أو حذفها. فهل لمزوّد الخدمة الحق في الاحتفاظ بالبيانات؟ وهل يملك العميل الحق المطلق في نقلها إلى مزوّد آخر؟ وماذا يحدث إذا تمّ تشفير البيانات ولا يملك العميل مفاتيح فك التشفير؟ كل هذه الأسئلة تظل محل جدل قانوني، ما لم تكن العقود السحابية قد تناولتها تفصيليًّا[٤].

---

(1) Seth D., Najana M. & Ranjan P. (2024). Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.68b5dea5.

(2) Adebola Folorunso, Olufunbi Babalola, Chineme Edgar Nwatu & Adebisi Adedoyin. (2024). A comprehensive model for ensuring data compliance in cloud computing environment. World Journal of Advanced Research and Reviews. Vol 24. Is 2. PP 1983–1995. https://doi.org/10.30574/wjarr.2024.24.2.3514.

(3) Rognstad O.-A. (2024). Data ownership' ambiguity. In Promoting Sustainable Innovation and the Circular Economy. Routledge. 1st Edition. PP 114–133. https://doi.org/10.4324/9781003309093-7.

(4) A. Sundararajan, G. Liu, M. Starke, R. K. Moorthy & C. Irwin. (2024). Networked Microgrid Ownership, Data, and Control Implications: Challenges and Open Questions. 2024 IEEE Power & Energy Society General Meeting (PESGM). Seattle, WA, USA. PP 1-5. doi: 10.1109/PESGM51994.2024.10688903.

٧ـ **الإخلال بشروط التعاقد والتزامات الخدمة**: الذي تُبنى عليه العلاقة بين المزوّد والعميل.

ويُعد الإخلال بهذه الاتفاقيات من أبرز أسباب النزاعات القانونية[١]، لا سيما في حالات[٢]:

- فقدان البيانات نتيجة عطل تقني أو اختراق أمني.
- انقطاع الخدمة لفترات تتجاوز الحدود المسموح بها.
- عدم الالتزام بمعايير الحماية والتشفير المتفق عليها.

في هذه الحالات، يُطالب العملاء غالبًا بتعويضات عن الأضرار المادية أو المعنوية التي لحقت بهم، ويواجه القاضي أو المحكّم تحديًا في تكييف العلاقة التعاقدية وتحديد المسؤولية بدقة، لا سيما في ظل التعقيد التقني للمسألة.

إن التحديات القانونية المرتبطة بالخدمات السحابية ليست مجرد مسائل نظرية، بل هي عقبات عملية تَعوق التبني الكامل للخدمات السحابية، وتُعرض الأفراد والمؤسسات لمخاطر جمة. إن التعامل الفعال مع هذه التحديات يتطلب نهجًا استباقيًّا يشمل[٣]:

١- **التشريع الذكي**: تطوير أطر قانونية وطنية ودولية أكثر مرونة وشمولية، قادرة على مواكبة التطور التكنولوجي، وتُقدم حلولًا واضحة لتضارب القوانين وقضايا الولاية القضائية.

٢- **العقود الشفافة والمفصلة**: يجب على العملاء إجراء "العناية الواجبة" الدقيقة عند اختيار مزودي الخدمات السحابية، والتفاوض على عقود واضحة تتناول بشكل صريح قضايا الولاية القضائية، أمن البيانات، المسؤولية، وشروط إنهاء الخدمة ونقل البيانات.

٣- **الامتثال الاستباقي**: على المؤسسات أن تُقيم باستمرار مدى امتثالها للوائح المحلية والدولية ذات الصلة بالخدمات السحابية، وأن تُطبق سياسات داخلية صارمة لإدارة البيانات.

---

(1) Merkin KC R., Saintier S. & Poole J. (2023). 13. Breach of contract. In Poole's Casebook on Contract Law. Oxford University Press. PP 638–687. https://doi.org/10.1093/he/9780192885081.003.0013.

(2) Hussein B. F., & Mahmoud I. A. (2024). The Legal Implications of a Food Service Provider's Breach of Obligations a Comparative Study. Journal of Ecohumanism. Vol 3. Is 8. PP 9967-9981. https://doi.org/10.62754/joe.v3i8.5609.

(3) Bala Akhileswar, A., Kumar Chelluboyina, Y., Vardhan Boya, H., Rao, K. V. & Siva Krishna C. N. (2024). An Analysis of Managing the Cloud: Obstacles and Solutions for Efficient Administration and Protection. International Journal of Innovative Science and Research Technology (IJISRT). Vol 9. Is 8. PP 2537–2544. https://doi.org/10.38124/ijisrt/ijisrt24aug1487.

٤- **التعاون الدولي**: ضرورة تعزيز التعاون بين الدول لتطوير اتفاقيات ومعاهدات دولية تُسهل تبادل المعلومات القانونية وتُقدم حلولًا متوازنة لتضارب القوانين في الفضاء السحابي.

تعكس التحديات القانونية المرتبطة بالخدمات السحابية الحاجة إلى مقاربة تشريعية مرنة ومتعددة المستويات، تراعي خصوصية التقنية، وتؤطر العلاقة بين الأطراف تعاقديًا وأمنيًا وقضائيًا. ومن المهم أيضًا الدفع نحو تنسيق دولي قانوني يُقلّل من تضارب التشريعات ويُعزّز مبادئ الثقة الرقمية، خاصة في ظل التحول العالمي نحو الاعتماد الكامل على البنية السحابية في الخدمات الحكومية، والمالية، والتعليمية. إذ لا يمكن فصل التطور التكنولوجي عن الإطار القانوني الذي يحكمه. إن بناء بيئة سحابية آمنة وموثوقة من الناحية القانونية هو مفتاح استدامة الابتكار وضمان الثقة في الاقتصاد الرقمي العالمي.

تحليل للتحديات القانونية المصرية والكويتية والاتحاد الأوروبي المرتبط بالخدمات السحابية:

إن استخدام الخدمات السحابية يثير تحديات قانونية معقدة سواء عند استخدام التخزين السحابي أو معالجة النزاعات المتعلقة به، إذ تتباين بحسب الأنظمة القانونية الوطنية والدولية. في هذا السياق، يُظهر القانون المصري، والقانون الكويتي، والتشريعات الأوروبية "خاصةً اللائحة العامة لحماية البيانات – GDPR" اختلافات جوهرية في تناول هذه التحديات. وفيما يلي تحليل لتلك التشريعات:

١ـ التحديات في ضوء القانون المصري[(١)]: نجد أن الدستور المصري من خلال (المادة ٥٧) التي تنص على أن خصوصية الحياة الخاصة للمواطن، وسرية مأذون بها للاتصالات والبيانات الشخصية لا يجوز المساس بها إلا بموجب نص دستوري أو قانون. وكل ذلك بشروط تتعلق بتحقيق المصلحة العامة، وبقرار قضائي مسبب في جرائم معينة ومحددة. وهذا يتماشى مع مبدأ المشروعية والتناسب المذكور في تقرير الأمم المتحدة.

---

(١) إنّ القانون المصري يحقق درجة جيدة من المطابقة لتوصيات الأمم المتحدة الواردة في A/HRC/39/29، مع تطابق واضح في المبادئ الجوهرية مثل المشروعية، والتدخل القضائي، والحقوق الفردية. ومع ذلك، فإن التحديات الفعلية تكمن في تطوير الآليات التنفيذية عبر تعزيز الرقابة والإجراءات التقنية المرافقة لتطبيق القانون، خصوصًا فيما يتعلق باستخدام الذكاء الاصطناعي والمراقبة الجماعية.

ويواجه التشريع المصري- شأنه شأن العديد من النظم القانونية المعاصرة- تحديات جمة في معالجة النزاعات المرتبطة بالتخزين السحابي. ويرجع هذا القصور في جانب كبير منه إلى طبيعة هذه التقنية العابرة للحدود وتطورها المتسارع الذي يفوق قدرة الأطر القانونية على المواكبة.

في هذا السياق، تبرز الحاجة المُلحة لضمان توافق التشريع المصري مع المعايير الدولية لحماية البيانات، التي لم تُدمج بشكل كافٍ حتى الآن. فمن الضروري إجراء حوارات شفافة وشاملة لكافة الأطراف المعنية، وهو ما لا يتوفر حاليًا بالقدر الكافي. كما يتطلب الأمر تضمين قائمة واضحة وملزمة لمبادئ حماية البيانات ضمن الإطار القانوني الوطني، إلى جانب تحديد الأساس القانوني صراحةً الذي يسمح بمعالجة البيانات.

علاوة على ذلك، يغيب عن التشريع المصري حاليًا إدراج قائمة شاملة وملزمة بحقوق المستخدمين في سياق التخزين السحابي، وهو ما يُعد فجوة قانونية تزيد من تعقيد النزاعات. كما أن تحديد نطاق واضح للتطبيق يُعد أمرًا ضروريًّا لفض تداخل الاختصاصات وضمان اليقين القانوني.

وتمُثل آليات نقل البيانات بشكل آمن إلى بلدان ثالثة تحديًا آخر، إذ تتطلب إنشاء آليات ملزمة وشفافة لحماية البيانات خلال هذه العمليات. وتبرز أهمية حماية أمن ونزاهة البيانات بشكل فعال، إلى جانب تطوير آليات لمنع انتهاك البيانات والإبلاغ عنها بشكل يُعزز الثقة في الخدمات السحابية.

كما يتطلب الأمر حتميًّا إنشاء سلطة مستقلة وآليات قوية لإنفاذ القانون تكون قادرة على التعامل مع تعقيدات النزاعات الرقمية، وهو ما يُعد نقطة ضعف في الإطار الحالي. بالإضافة إلى ضرورة ضمان استمرارية حماية البيانات والخصوصية لتقديم بيئة قانونية لخدمات التخزين السحابي في مصر.

كما لا يوجد في مصر حتى الآن قانون موحّد أو إطار تشريعي صريح ينظم عمل الخدمات السحابية، وإذا كان هناك نزاع محدد حول تلك الخدمات. ولذلك يتم الاستناد إلى القوانين العامة لتنظيم العمل، مثل:

أ- قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨.

ب- قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠[١].

---

(١) قانون حماية البيانات الشخصية رقم ١٥١/ ٢٠٢٠:

- يفرض قواعد واضحة لجمع، معالجة، ومشاركة البيانات الشخصية.
- يتطلب موافقة صريحة، ويعطي الأفراد حق الوصول، التصحيح، والحذف.
- يعاقب على انتهاكات الخصوصية بغرامات وسنوات حبس.

وهذا ينسجم مع التوصيات العالمية حول تأطير استخدام البيانات ضمن نظام قانوني محكم.

فالمبادئ الدولية (UN) تركز على الحاجة إلى ضبط استخدام التقنيات كالأتمتة والذكاء الاصطناعي لضمان الحقوق الشخصية[١]، والتشريع المصري السابق يأتي مواكبًا في تحديد الشروط القانونية للتدخل في الخصوصية، وإن كانت التحديات تكمن في التنفيذ والرقابة والممارسة الفعلية في الواقع العملي[٢]. فلم يعتمد القانون المصري بشكل كامل على المعايير الدولية مثل الـGDPR، ما يجعل الشركات متعددة الجنسيات تواجه صعوبة في الامتثال للتشريعات الوطنية[٣].

٢- **التحديات في ضوء القانون الكويتي**: يواجه التشريع الكويتي، كغيره من النظم القانونية في ظل التطور التكنولوجي المتسارع، تحديات ملحوظة في معالجة النزاعات الناشئة عن خدمات التخزين السحابي. فلا يزال القانون الكويتي يفتقر إلى تعريف قانوني واضح ومحدد للتخزين السحابي بوصفه خدمة تقنية، مما يُصعب تكييف العلاقة بين مزود الخدمة والعميل. هل هي علاقة إيجار، أم خدمة، أم عقد من نوع خاص؟ هذا الغموض يؤثر على تحديد حقوق والتزامات الأطراف، خاصة في حال وقوع نزاعات.

بما أن التخزين السحابي ينطوي على طبيعة عابرة للحدود (قد تكون الخوادم في دول مختلفة)، فإن تحديد المحكمة المختصة بنظر النزاع والقانون الواجب التطبيق يُمثل تحديًا كبيرًا. وعلى الرغم من وجود لائحة حماية خصوصية البيانات الصادرة عن الهيئة العامة للاتصالات وتقنية المعلومات (CITRA) في الكويت، فإن تطبيقها على التخزين السحابي يثير تساؤلات، خاصة فيما يتعلق بنقل البيانات إلى بلدان ثالثة التي قد لا تملك نفس مستوى الحماية. التحدي يكمن في ضمان التوافق مع المعايير الدولية لحماية البيانات وكيفية تطبيقها على مقدمي الخدمات السحابية العالميين.

فتحديد مسؤولية مزود خدمة التخزين السحابي عن فقدان البيانات، تلفها، اختراقها، أو إساءة استخدامها يُعد أمرًا معقدًا. فالعقود المبرمة (غالبًا عقود إذعان) قد تُحاول إخلاء مسؤولية المزود أو

---

(١) مجلس حقوق الإنسان. (٢٠١٨). تقرير المفوّض السامي للأمم المتحدة حول "الحق في الخصوصية في عصر الرقمنة" (A/HRC/39/29). للأمم المتحدة. ومتاح من خلال الرابط التالي: https://docs.un.org/ar/A/HRC/39/29. وتم الاطلاع عليه بتاريخ ٥/ ٧/ ٢٠٢٥.

(٢) سيد أحمد محمود. (٢٠٢٤). حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري رقم ١٥١ لسنة ٢٠٢٠ (حماية البيانات الشخصية المعالجة إلكترونيًا) بين الواقع والمأمول. مجلة العلوم القانونية والاقتصادية. مجلد ٦٦. عدد ١. الصفحات ١٤٣٩-١٤٨٢. doi: 10.21608/jelc.2024.341026

(٣) المرجع السابق. الصفحات ١٤٣٩-١٤٨٢.

تحديدها بشكل كبير، مما قد يَضُر بمصالح المستخدمين. يتطلب الأمر نصوصًا قانونية واضحة تُحدد مدى هذه المسؤولية، خاصة في حالات الإهمال الجسيم أو التعمد.

على الرغم من وجود قانون مكافحة جرائم تقنية المعلومات (القانون رقم ٦٣ لسنة ٢٠١٥)، الذي يجُرم بعض الأفعال المتعلقة بالوصول غير المصرح به أو التلاعب بالبيانات، فإن التحدي يكمن في تطبيق هذه النصوص على البيئة السحابية المعقدة. تتطلب حماية أمن ونزاهة البيانات في السحابة آليات تقنية وقانونية أكثر تفصيلًا، بما في ذلك تطوير آليات لمنع الانتهاكات والإبلاغ عنها بفعالية.

ولا تزال حقوق المستخدمين فيما يتعلق بالتحكم ببياناتهم المخزنة (مثل حق الوصول، التصحيح، الحذف، ونقل البيانات) بحاجة إلى تعزيز قانوني صريح، خاصة عند وجود أو نشوء النزاعات. كما أن مسألة الوصول إلى البيانات المخزنة لأغراض إنفاذ القانون (كالتحقيقات الجنائية) تثير تحديات تتعلق بالسيادة الوطنية، خاصة إذا كانت البيانات مخُزنة خارج الدولة.

فهناك حاجة إلى إنشاء سلطة مستقلة ذات صلاحيات قوية للإشراف على حماية البيانات وإنفاذ القوانين المتعلقة بها، والتصدي للنزاعات في البيئة الرقمية، وهو ما قد لا يكون متوافرًا بالكامل في الهياكل الحالية.

باختصار، يواجه التشريع الكويتي ضرورة ملحة لتطوير إطار قانوني شامل ومتخصص لمعالجة النزاعات المتعلقة بالتخزين السحابي، بما يضمن حماية حقوق الأفراد، ويحدد مسؤوليات الأطراف، ويواكب التطورات التقنية مع الالتزام بالمعايير الدولية.

فالقانون الكويتي لا يتضمن تشريعًا خاصًّا ينظم الخدمات السحابية أو حتى النزاعات المتعلقة بها. ولذلك يتم اللجوء إلى أحكام القوانين العامة[1]، مثل:

---

(١) القانون الكويتي لا يتضمن تشريعًا خاصًّا ينظم الخدمات السحابية بشكل مستقل، وإنما يتم اللجوء إلى أحكام القوانين العامة ذات الصلة، خاصة قانون إنشاء الهيئة العامة للاتصالات وتقنية المعلومات رقم ٣٧ لسنة ٢٠١٤ المعدل بقانون ٩٨ لسنة ٢٠١٥، فقد أصدرت الهيئة قرارات تنظيمية مثل قرار رقم ١١٢ لسنة ٢٠٢٠ بشأن الإطار التنظيمي للحوسبة السحابية الذي ينظم عمل مقدمي خدمات الحوسبة السحابية والجهات المستخدمة لها في الكويت.

والهيئة العامة للاتصالات وتقنية المعلومات في الكويت بدأت بمنح تراخيص محلية لمقدمي خدمات الحوسبة السحابية، فقد تم منح ٨ تراخيص حتى الآن مع تحضيرات لمنح ٤ أخرى، وذلك بهدف حفظ البيانات الحكومية والقطاع الخاص داخل مراكز بيانات محلية لضمان أمن البيانات ورفع مستوى الحماية، خصوصًا للبيانات الحساسة التي بات ممنوعًا تخزينها خارج الكويت.

أ- قانون مكافحة جرائم تقنية المعلومات رقم ٦٣ لسنة ٢٠١٥.

ب- قانون المعاملات الإلكترونية رقم ٢٠ لسنة ٢٠١٤.

- **التعامل مع البيانات الشخصية**[1]: لا يوجد قانون شامل لحماية البيانات الشخصية (على غرار اللائحة الأوروبية). يُثار تحدٍّ كبير أمام الشركات العاملة بالكويت، خاصة في ظل تصاعد أهمية البيانات الشخصية.

- **تحدي تنازع القوانين**: نظرًا لكون بيانات المستخدم قد تُخزّن في خوادم خارج الكويت، يصعب أحيانًا تحديد الجهة القضائية المختصة أو القانون الواجب التطبيق.

٣- **التحديات وفقًا للتشريعات الأوروبية (GDPR)**: تشكل اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي الإطار المرجعي الأكثر صرامة وشمولًا في حماية البيانات الشخصية في العالم، وتُطبّق على أي جهة تقوم بمعالجة بيانات تخص أشخاصًا داخل

كما تركز الكويت على تعزيز الأمن السيبراني في بيئة الحوسبة السحابية، من خلال تطبيق ضوابط أمنية وإرشادات مستمدة من معايير دولية مثل ISO/IEC 27017، الذي يحدد مسؤوليات مزودي الخدمات والمستخدمين، ويعزز حماية البيانات السحابية من الوصول غير المصرح به أو الفقد أو التلاعب.

بالتالي، على الرغم من غياب تشريع خاص منفصل، هناك تنظيمات وإجراءات تنظيمية صادرة عن الهيئة العامة للاتصالات وتقنية المعلومات تنظم عمل الحوسبة السحابية في الكويت، مع التركيز على الترخيص المحلي، حماية البيانات، وضمان الأمن السيبراني.

ينظر؛ الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي: https://citra.gov.kw/sites/ar/Pages/ServiceDetails.aspx?SrvcID=93. وتم الاطلاع عليه بتاريخ ١٥/ ٥/ ٢٠٢٥.

(١) الكويت، مثل العديد من الدول، اتجهت نحو تعزيز أطرها القانونية لحماية البيانات الشخصية لمواكبة التطورات العالمية ومعايير الخصوصية. لم يكن لدى الكويت في السابق قانون شامل ومستقل لحماية البيانات الشخصية يُطبق على جميع الأشخاص الاعتباريين والطبيعيين بشكل عام. بدلًا من ذلك، كانت هناك أحكام متفرقة في قوانين مختلفة تتعلق بخصوصية البيانات. ومع ذلك، شهدت الكويت مؤخرًا تطورًا مهمًّا في هذا المجال.

تُعد الهيئة العامة للاتصالات وتقنية المعلومات (CITRA) الجهة المسؤولة عن إنفاذ هذه اللائحة في الكويت. تتمتع الهيئة بصلاحية التحقيق في أنشطة معالجة البيانات، وإصدار التحذيرات، وفرض الامتثال، وتطبيق العقوبات.

تُكمل هذه اللائحة أحكامًا أخرى ذات صلة موجودة في تشريعات كويتية أخرى مثل القانون رقم ٢٠ لسنة ٢٠١٤ بشأن المعاملات الإلكترونية، الذي يتضمن بعض الأحكام المتعلقة بخصوصية البيانات والسجلات الإلكترونية. كما يتكامل مع القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات، الذي يجُرم بعض الأفعال المتعلقة بالوصول غير المصرح به للبيانات والمعلومات.

الاتحاد الأوروبي، بغض النظر عن مكان وجود مقدم الخدمة. وبذلك تمتد آثارها إلى مزوّدي خدمات التخزين السحابي، سواء داخل أوروبا أو خارجها، ما دامت الخدمات تستهدف المستخدمين الأوروبيين.

فقد أصدرت محكمة العدل الأوروبية (CJEU) في قضية Schrems II (2020) حكمًا بارزًا ألغى اتفاقية Privacy Shield بين الاتحاد الأوروبي والولايات المتحدة، معتبرة أن القوانين الأمريكية لا توفر حماية كافية للبيانات الأوروبية. وقد أدى هذا الحكم إلى مضاعفة المسؤوليات على الشركات السحابية، وارتفاع النزاعات بشأن التوافق مع شروط نقل البيانات[١].

أصدر الاتحاد الأوروبي اللائحة العامة لحماية البيانات (GDPR)، التي تُعد الأكثر شمولًا عالميًّا. تُحدد هذه اللائحة قواعد صارمة لمعالجة البيانات، بما يشمل[٢]:

أ- مبدأ الشفافية.

ب- الحقوق الصريحة للأفراد (الحق في النسيان، الحق في التصحيح، إلخ).

ت- التزامات واضحة لمزوّدي الخدمات السحابية.

- **تحديات الامتثال الصارم**: يواجه مزودو الخدمات السحابية تحديًا في الامتثال للمعايير الصارمة للـGDPR، خاصةً فيما يخص نقل البيانات خارج الاتحاد الأوروبي.

- **مسؤولية المعالجة**: تُحدّد GDPR- بوضوح المسؤولية بين "المتحكّم بالبيانات" و"معالج البيانات"، وتفرض عقوبات صارمة على المخالفين.

أظهر تطبيق اللائحة العامة لحماية البيانات مدى تعقيد الإطار القانوني لعقود التخزين السحابي، خاصة عندما يتداخل فيه البعد التعاقدي مع التزامات تنظيمية صارمة. ويمثل التحدي الرئيس في إيجاد توازن بين المرونة التقنية التي توفرها الحوسبة السحابية، والضمانات القانونية لحماية

---

(1) Drechsler L. & Kamara I. (2022). "Chapter 13: Essential equivalence as a benchmark for international data transfers after Schrems II". In Research Handbook on EU Data Protection Law. Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00022.

(2) Ashwini Kumar. (2023). The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis. International Journal For Multidisciplinary Research. Voll 5. Is 2. https://doi.org/10.36948/ijfmr.2023.v05i02.2534.

الخصوصية، وهو ما يجعل الالتزام الصارم بـ GDPR ضروريًّا لتفادي النزاعات والتعرض للعقوبات.

يتّضح من هذه المقارنة أن بيئة الاتحاد الأوروبي، بفضل GDPR-، توفر إطارًا متقدّمًا وشاملًا لحماية البيانات ومعالجة النزاعات المرتبطة بالخدمات السحابية. في المقابل، ما زال القانون المصري والكويتي بحاجة إلى تطوير تشريعات خاصة بالسحابة، أو على الأقل تبني مبادئ أساسية مستمدة من المعايير الدولية.

العقود في التخزين السحابي "طبيعتها وتداعياتها القانونية":

تُعد عقود التخزين السحابي من العقود الحديثة ذات الطبيعة المركّبة، التي تجمع بين عناصر متعددة تشمل تقديم خدمات تقنية، نقل بيانات، معالجة معلومات، وأحيانًا توفير أمن سيبراني. وغالبًا ما تتخذ هذه العقود شكل عقود إذعان إلكترونية[١]، بكونها أحادية الجانب، إذ يفرض فيها مزود الخدمة شروطه دون أن يمتلك المستخدم (الطرف الأضعف) أي قدرة على التفاوض عليها، مما يثير إشكاليات قانونية جوهرية تتعلق بحرية الإرادة وتوازن الالتزامات التعاقدية[٢].

تميل الشركات المقدِّمة خدمات السحابة إلى استخدام عقود نمطية موحّدة، تُفرض من جانب واحد، وتُبرم بوسائل إلكترونية دون تواصل مباشر، مما يجعلها أقرب إلى عقود التجارة الدولية من حيث الشكل، ولكنها تفتقر إلى التوازن الحاصل في العقود التقليدية.

- **الطبيعة القانونية للعقد**: يمكن تصنيف عقد التخزين السحابي إلى[٣]:

١- عقد تقديم خدمة (Service Contract)، لكونه يقوم على التزام بتوفير قدرة تخزينية أو برمجيات عن بُعد.

٢- عقد ترخيص باستخدام برنامج (License Agreement)، حين تشمل الخدمة إتاحة استخدام برامج مملوكة لمزوّد الخدمة.

---

(١) عقد الإذعان هو نوع من العقود يقبل فيه أحد الطرفين الشروط الجاهزة التي يضعها الطرف الأقوى، دون أن تكون له فرصة لمناقشة هذه الشروط أو تعديلها. في سياق التخزين السحابي، يُوافق المستخدم على الشروط والأحكام التي يُمليها مزود الخدمة، وهي تحدد بشكل قاطع حقوقه وواجباته، فضلاً عن نطاق مسؤولية مزود الخدمة وحدودها.

(٢) صفاء شكور عباس. (٢٠٢٠). التنظيم القانوني للعقود المركبة في القانون المدني. مجلة الدراسات المستدامة. مجلد ٢. عدد ١. الصفحات ٢١٥-٢٣٠.

(3) Khan A.Q., Matskin M., Prodan R. et al. (2024). Cloud storage cost: a taxonomy and survey. World Wide Web. Vol 27. article number 36. https://doi.org/10.1007/s11280-024-01273-4.

٣- عقد وديعة إلكترونية (Digital Bailment)، في حال احتفظ المزود بالبيانات دون التصرّف فيها.

٤- عقد مختلط أو غير مسمّى، نظرًا لتركيبته التي لا تخضع لتعريف عقد تقليدي وحيد.

هذا التعدّد في الطبيعة القانونية يُصعّب عملية التكييف القانوني للنزاعات الناشئة، مما يضع القاضي أو المحكِّم أمام تحدي تحديد الإطار القانوني المنطبق على العلاقة التعاقدية.

- **الآثار القانونية والتحديات التعاقدية**[١]:

١ـتحديد القانون الواجب التطبيق: بسبب الطبيعة العابرة للحدود لهذه العقود، غالبًا ما يُثار النزاع حول القانون الوطني الواجب التطبيق، لا سيما إذا لم يتم النص عليه صراحة في العقد. وتبرز الحاجة إلى قواعد إسناد واضحة لحسم هذا التنازع.

٢ـ الإخلال بالتزامات أمن البيانات: يُثير الإخلال بمستوى الحماية المتفق عليه للبيانات، أو تسريبها، مسؤولية تعاقدية جسيمة، قد تصل في بعض التشريعات إلى المسؤولية التقصيرية، لا سيما إذا ارتبط الفعل بخطأ جسيم أو إهمال واضح من المزود.

٣ـ تحديد الجهة المسؤولة في حالة تعدد الأطراف: في بيئات الحوسبة السحابية المعقّدة، قد تتداخل المسؤوليات بين المزود الرئيس والموزّعين أو المزوّدين من الباطن، مما يخلق تعقيدًا في تتبع المسؤولية القانونية.

٤ـشرط التحكيم وتقييد الحق في التقاضي: كثيرًا ما تحتوي عقود التخزين السحابي على شرط تحكيمي أو تحديد لجهة قضائية في بلد أجنبي، وهو ما يُعد عائقًا عمليًّا للمستخدم العادي أو المؤسسات الصغيرة في حال نشوء نزاع.

٥ـ عدم وضوح شروط إنهاء العقد وحذف البيانات: تفتقر كثير من العقود إلى آلية واضحة تنظم استرداد البيانات أو حذفها بشكل آمن عند إنهاء العلاقة التعاقدية، مما يفتح الباب أمام سوء الاستخدام أو الابتزاز التكنولوجي.

---

(١) إيهاب محمد سعيد محمود عويضة العماوي. (٢٠٢٢). القانون الواجب التطبيق على عقود التجارة الدولية. المجلة القانونية. مجلد ١٤. عدد ٦. الصفحات ١٩١٣-١٩٦٦.

https://doi.org/10.21608/jlaw.2022.269930.

تلعب عقود الإذعان دورًا حاسمًا في تنظيم علاقة المستخدمين بمزودي خدمات التخزين السحابي. ومع ذلك، من الضروري دراسة هذه العقود بعناية فائقة، مع الأخذ في الاعتبار أهمية تحقيق توازن عادل بين حماية حقوق المستخدمين وصيانة مصالح مزودي الخدمة.

- **تنظيم عقود الخدمات السحابية (SLAs):**

١- **الاتحاد الأوروبي**: لا يوجد قانون مُحدد يُنظم عقود SLA بذاتها، ولكن GDPR يفرض متطلبات معينة على محتوى العقود بين المتحكم والمعالج (المادة ٢٨)[١]، مثل ضرورة تحديد موضوع ومدة المعالجة، طبيعتها وغرضها، نوع البيانات الشخصية، فئات أصحاب البيانات، وحقوق والتزامات الطرفين. كما أن توجيهات الاتحاد الأوروبي تُشجع على استخدام بنود تعاقدية قياسية[٢].

٢- **مصر والكويت**: لا توجد تشريعات مُحددة تُفصّل متطلبات عقود الخدمات السحابية. تخضع هذه العقود للأحكام العامة للقانون المدني في كل بلد. ومع ذلك، فإن قوانين حماية البيانات الشخصية الجديدة ستفرض بشكل غير مباشر ضرورة تضمين بنود متعلقة بأمن البيانات، والخصوصية، ونقل البيانات، والالتزام باللوائح. يجب على الأطراف التأكد من أن هذه العقود تُقدم ضمانات كافية للعميل.

وعلى العكس من ذلك، يرى البعض أن عدم وجود قوانين محددة تحكم اتفاقيات مستوى الخدمة (SLAs) قد يؤدي إلى الغموض في الامتثال، مما قد يقوض فعالية أحكام اللائحة العامة

---

(١) **المتطلبات الرئيسة للمادة ٢٨:**

- **موضوع المعالجة**: يجب أن تحدد العقود بوضوح أنواع البيانات الشخصية التي تتم معالجتها، مما يضمن الشفافية والمساءلة.
- **مدة المعالجة**: يجب أن يحدد العقد المدة التي ستتم فيها معالجة البيانات، وهو أمر بالغ الأهمية للامتثال لمبادئ تقليل البيانات.
- **التزامات إضافية**: تتطلب اللائحة العامة لحماية البيانات من المعالجين تنفيذ التدابير الفنية والتنظيمية المناسبة لحماية البيانات، وكذلك لمساعدة وحدات التحكم في الوفاء بالتزاماتها بموجب اللائحة.

(2) Dobrilă M.-C. (2021). Aspecte teoretice şi jurisprudenţiale privind respectarea GDPR la încheierea şi executarea unui contract. ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI (SERIE NOUĂ). ŞTIINŢE JURIDICE. Vol 67. Is 2. PP 93–106. https://doi.org/10.47743/jss-2021-67-4-6.

لحماية البيانات. وهذا يسلط الضوء على الحاجة إلى أطر قانونية أوضح لدعم تنفيذ اللائحة العامة لحماية البيانات في سياقات مختلفة[1].

تُظهر المقارنة بين القانون المصري، الكويتي، والاتحاد الأوروبي تفاوتًا في التعامل مع التحديات القانونية للخدمات السحابية. يتفوق الاتحاد الأوروبي بفضل GDPR ومعايير الأمان الصارمة، بينما تعاني مصر والكويت من فجوات في التشريعات والتطبيق. مصر متقدمة على الكويت بقانون حماية البيانات، لكن كليهما يحتاج إلى تعزيز البنية التحتية والتوعية. من خلال تبني تشريعات شاملة. كما يُبرز هذا المجال أهمية التوازن بين الابتكار والحماية القانونية، فكما قال ويليام جيبسون: "المستقبل هنا بالفعل، لكنه لم يُوزع بعد بشكل عادل".

(1) 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. Is 1. https://doi.org/10.1093/jlb/lsab007.

المبحث الثالث
القانون الواجب التطبيق وطرق فض النزاعات التخزين السحابي

أصبحت تقنيات الحوسبة السحابية وسيلة أساسية لتخزين ومعالجة البيانات في القطاعات الحكومية والخاصة على حدٍّ سواء. ومع هذا التطور التكنولوجي المتسارع، ظهرت إشكاليات قانونية متعددة، من أبرزها: تحديد الجهة القضائية المختصة والقانون الواجب التطبيق على النزاعات التي تنشأ عن العلاقات التعاقدية أو الأضرار الناجمة عن استخدام خدمات التخزين السحابي، خاصة في ظل الطبيعة العابرة للحدود لهذه الخدمات، والافتقار في كثير من الأحيان إلى موطن مادي واضح لمزوّد الخدمة أو لمكان تنفيذ الالتزامات.

فتنازع القوانين واختصاص المحاكم من أكثر المسائل تعقيدًا في هذا السياق، لا سيما أن العقود السحابية غالبًا ما تُبرم إلكترونيًّا، وتتضمن شروطًا نمطية يفرضها مزود الخدمة، تشمل اختيار القانون الواجب التطبيق أو شرط التحكيم. ومع ذلك، فإن هذه الشروط قد تُثار بشأنها عدة تحديات من حيث مشروعيتها، أو مدى توافقها مع النظام العام في الدولة التي يُطلب تنفيذ الحكم فيها، أو عندما يكون الطرف المتضرر مستهلكًا أو جهة حكومية غير قادرة على مجاراة مراكز التحكيم الأجنبية.

من جهة أخرى، فإن النزاعات المتعلقة بالتخزين السحابي لا تقتصر فقط على العقود، بل تشمل أيضًا جوانب المسؤولية التقصيرية عن فقدان البيانات، أو تسريبها، أو خرق الخصوصية، مما يطرح سؤالًا إضافيًّا حول القانون الموضوعي الذي يحكم هذه المسؤولية، خاصة إذا لم يتضمن العقد نصًّا صريحًا بهذا الخصوص، أو إذا وقع الفعل الضار خارج نطاق العلاقة التعاقدية.

وتزداد أهمية هذه الإشكالية مع غياب تنظيم تشريعي خاص في العديد من الدول العربية، ما يضطر القضاء أو هيئات التحكيم إلى الاستعانة بالقواعد العامة في القانون المدني أو التجاري، أو بالاتفاقيات الدولية الخاصة بالتجارة الإلكترونية وبتنازع القوانين، وهو ما يؤدي إلى نتائج قانونية متباينة في ظل اختلاف المعايير الوطنية لتحديد مكان الضرر، أو محل تنفيذ العقد، أو موقع الخوادم السحابية التي قد تكون موزعة بين عدة دول.

المطلب الأول
القانون الواجب التطبيق على نزاعات التخزين السحابي

مع ازدياد الاعتماد على خدمات التخزين السحابي في القطاعات العامة والخاصة، برزت تساؤلات قانونية متعلقة بالنزاعات التي تنشأ عن هذه الخدمات، لاسيما في ظل الطبيعة اللامادية والعابرة للحدود لهذه التقنية. ومن أهم هذه التساؤلات: ما هو القانون الذي يُطبّق على النزاع الناشئ عن عقد سحابي؟ وهل يمكن للأطراف فرض قانون معين؟ وما حدود ذلك في ضوء النظام العام الوطني؟

ووفقًا للمبدأ العام في القانون الدولي الخاص، والمادة ١٩ من القانون المدني المصري، يُسمح للأطراف باختيار القانون الذي يحكم العقد، شريطة ألا يُخالف هذا القانون النظام العام المصري أو أي قواعد آمرة.

وغالبًا ما تتضمن العقود السحابية بندًا يحدد القانون الواجب التطبيق (مثل القانون الإنجليزي أو الأمريكي)، لكن إرادة الأطراف ليست مطلقة، خاصة إذا تعلق الأمر بمستهلكين أو جهات إدارية وطنية، إذ يمكن لمحاكم بعض الدول تجاهل هذا الاتفاق إذا تعارض مع المصلحة العامة أو شكل إخلالًا بالتوازن العقدي[١].

إذا لم يُحدد القانون الواجب التطبيق في العقد، فإن قواعد الإسناد (conflict of laws) هي التي تُستخدم لتحديده. ووفقًا للتوجهات الحديثة، يمكن النظر في[٢]:

- مكان تنفيذ الالتزام الجوهري في العقد (وغالبًا ما يكون الدولة التي يقيم فيها المستخدم النهائي).
- موطن المدعى عليه أو مقر مزود الخدمة.
- القانون الأقرب صلة بالعقد.

ومع ذلك، فإن تعقيد بنية الخدمات السحابية يجعل من الصعب تطبيق هذه المعايير دون غموض، خاصة مع وجود خوادم متعددة موزعة عالميًا.

---

(١) أحمد جعفر شاوي. (٢٠٢٠). معايير تحديد القانون الواجب التطبيق على عقود الاستهلاك – دراسة مقارنة. مجلة كلية القانون والعلوم السياسية. العدد السادس. الصفحات ٢٠٩ – ٢٤١.
https://doi.org/10.61279/vrz1pf56 .

(٢) المرجع السابق.

حتى مع وجود اتفاق على قانون معين، يمكن لمحكمة الدولة التي يُطلب فيها تنفيذ حكم أو البت في النزاع، أن ترفض تطبيق القانون المختار إذا:

-تضمن أحكامًا تخُل بالحقوق الأساسية للمستخدمين (مثل حرية الوصول للبيانات، أو حماية الخصوصية).

-خالف القواعد الآمرة المتعلقة بحماية البيانات أو الأمن السيبراني، وهي مسائل تُعد من النظام العام في بعض الدول.

وقد كرس القضاء المصري هذا التوجه في العديد من الأحكام التي استبعدت تطبيق قوانين أجنبية في حال تعارضها مع المبادئ الأساسية للنظام القانوني الوطني[١].

مبادئ تحديد القانون الواجب التطبيق:

يُعد تحديد القانون الواجب التطبيق (Lex Causae) على نزاعات التخزين السحابي من أكثر المسائل القانونية في العصر الرقمي تعقيدا ، وذلك نظرًا للطبيعة العابرة للحدود لخدمات التخزين السحابي، وغياب الوجود المادي الملموس لموقع تخزين البيانات، وتعدد الأطراف المعنية (المستخدم، مزود الخدمة، ومزودو الخدمة الباطنيون). لا توجد حتى الآن اتفاقيات دولية شاملة أو قوانين وطنية موحدة تُحدد بشكل قاطع القانون الواجب التطبيق على هذه النزاعات، مما يُدخلها في نطاق قواعد تنازع القوانين التقليدية، التي قد لا تكون مُهيأة بالكامل لخصوصية البيئة الرقمية[٢].

وفي غياب نص قانوني صريح، تعتمد المحاكم وهيئات التحكيم على مجموعة من المبادئ والآليات لتحديد القانون المناسب، أبرزها[٣]:

---

(١) محمد محمود على. (٢٠٢٢). تنازع القوانين في مجال إنفاذ اتفاقات التسوية التجارية الدولية طبقاً لمعاهدة سنغافورة للوساطة ٢٠١٨. المجلة الدولية للفقه والقضاء والتشريع. مجلد ٣. عدد ١. الصفحات ١-٣١.

(٢) محمد عبدالقادر حفني الخطيب. (٢٠٢٤). حرية الأطراف في اختيار القانون الواجب التطبيق على منازعات عقود الوكالة التجارية الدولية. مجلة البحوث القانونية والاقتصادية، تصدر عن كلية الحقوق ـ جامعة المنصورة. مجلد ١٤، عدد ٨٧. الصفحات ١-٤٨. https://doi.org/10.21608/mjle.2024.343026.

(٣) فاطمة الزهراء رباح، بشرى عمور. دور المحكم في تحديد القانون الواجب التطبيق على موضوع النزاع. دفاتر البحوث العلمية. مجلد ١١، عدد ١. الصفحات ٣٥٥-٣٧٣.

https://asjp.cerist.dz/en/article/221872.

١ـ**اختيار الأطراف** (Party Autonomy): يُعد مبدأ سلطان الإرادة هو الأساس. يحق للأطراف المتعاقدة (المستخدم ومزود الخدمة) اختيار القانون الذي يحكم عقدهم والنزاعات الناشئة عنه. هذا الاختيار يجب أن يكون صريحًا وواضحًا في عقد الخدمة. تُعد هذه البنود سارية ونافذة، ما لم تتعارض مع النظام العام أو القواعد الآمرة في الدولة التي يُنظر فيها النزاع (دولة القاضي أو المحكِّم). يُعد هذا الخيار هو الأفضل لتحقيق اليقين القانوني.

٢ـ **غياب اختيار الأطراف**: في حال عدم وجود اتفاق صريح على القانون الواجب التطبيق في العقد، تلجأ المحكمة أو هيئة التحكيم إلى تطبيق قواعد تنازع القوانين في محفل النزاع (Lex Fori). هذه القواعد تختلف من دولة لأخرى، وعادةً ما تَبحث عن "العلاقة الأكثر ارتباطًا" بالعقد أو النزاع. في سياق التخزين السحابي، قد تُثير هذه العلاقة إشكاليات:

-**مكان إبرام العقد**: قد يكون إلكترونيًا ولا يُحدد مكانًا ماديًا واضحًا.

-**مكان تنفيذ الالتزام الرئيس**: وهو تقديم خدمة التخزين، التي تُقدم عبر خوادم قد تكون في دول متعددة.

-**محل إقامة أو جنسية الأطراف**: يُمكن أن تكون مختلفة بين المستخدم ومزود الخدمة.

-**مكان وجود الخوادم**: يُعد هذا عاملًا مهمًا، لكنه قد يكون متغيرًا أو مجهولًا للمستخدم، وقد لا يكون ذا صلة مباشرة بمحل إقامة العميل أو جنسيته.

٣ـ **مبدأ بلد المنشأ ومبدأ بلد الوجهة**: تُستخدم هذه المبادئ في سياق التجارة الإلكترونية والخدمات الرقمية.

-بلد المنشأ: يُطبق قانون الدولة التي يقع فيها مزود الخدمة.

-بلد الوجهة: يُطبق قانون الدولة التي يوجد فيها المستهلك/ المستخدم.

يُفضل للائحة العامة لحماية البيانات مبدأ "مكان التأسيس" الذي يميل إلى تطبيق قانون الاتحاد الأوروبي، حتى لو كان المزود خارج الاتحاد، إذا كان يقدم خدمات لمواطنيه.

٤ـ**قواعد تنازع القوانين الخاصة بحماية المستهلك**: تميل العديد من التشريعات الحديثة إلى حماية المستهلك (الطرف الأضعف). لذا، ففي نزاعات التخزين السحابي التي يكون أحد أطرافها

مستهلكًا، قد تُطبق قواعد تنازع القوانين التي تُشير إلى قانون بلد إقامة المستهلك، حتى لو اختار الأطراف قانوناً آخر، وذلك لحماية القواعد الآمرة المتعلقة بحماية المستهلك في تلك الدولة.

٥- أهم العقبات في هذا السياق:

-**تجريد الموقع الجغرافي للبيانات**: من الصعب تحديد "موقع" البيانات المخزنة بدقة، فيمكن أن تنتشر عبر خوادم متعددة في دول مختلفة. هذا يُعقد من تطبيق قواعد تنازع القوانين التقليدية.

-**قوانين الولاية القضائية خارج الحدود**: مثل قانون CLOUD Act الأمريكي، الذي يسمح للسلطات الأمريكية بالوصول إلى بيانات الشركات الأمريكية، حتى لو كانت مخزنة خارج الولايات المتحدة. هذا يُمكن أن يُنشئ تضاربًا في القوانين والالتزامات بين قانون الدولة التي توجد بها الخوادم وقانون الدولة التي يتبعها المزود.

-**التعقيد الفني للعقود**: عقود التخزين السحابي غالبًا ما تكون معقدة فنيًّا وقانونيًّا، وقد تحتوي على بنود غير واضحة حول القانون الواجب التطبيق أو الاختصاص القضائي، مما يُصعب على القاضي غير المتخصص فهمها وتطبيقها.

في ظل المشهد القانوني الحالي، يبقى اختيار الأطراف للقانون الواجب التطبيق في عقد خدمة التخزين السحابي هو النهج الأكثر فعالية لضمان اليقين القانوني. ومع ذلك، يجب أن يكون هذا الاختيار متوافقًا مع القواعد الآمرة والنظام العام للدولة التي يُحتمل أن يُنظر فيها النزاع. في غياب هذا الاختيار، تُصبح المسألة معقدة وتعتمد على قواعد تنازع القوانين المحلية، التي قد تحتاج إلى تطوير لتواكب خصوصيات الخدمات السحابية.

القانون الواجب التطبيق على نزاعات التخزين السحابي:

١- **في القانون المصري**: تنص المادة (١٩) من القانون المدني على أنه "يسري على الالتزامات التعاقدية قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين، فإذا اختلفا موطنًا سري قانون الدولة التي تم فيها العقد، هذا ما لم يتفق المتعاقدان أو يتبين من الظروف تطبيق قانون آخر."، وبناءً على ذلك، يعتمد المشرّع المصري مبدأ إرادة المتعاقدين قاعدة أساسية في تحديد القانون الواجب التطبيق. فإذا نص العقد الإلكتروني "بما في ذلك عقد التخزين السحابي" على خضوعه لقانون معين، وجب احترام هذا الاختيار، شريطة ألا يتعارض مع النظام العام أو الآداب في مصر.

أما في حالة غياب الاختيار الصريح أو الضمني، فيتم اللجوء إلى معيار الدولة التي أُبرم فيها العقد أو التي يُفترض أنها الأكثر ارتباطًا به. إلا أن تطبيق هذه القواعد في بيئة رقمية يثير صعوبات واقعية، نظرًا لأن العقد الإلكتروني لا يُبرم في "مكان مادي" محدد، بل عبر خوادم وشبكات عابرة للدول، وهو ما يجعل تحديد "مكان إبرام العقد" مفهومًا افتراضيًّا أكثر منه عمليًّا.

كما يجوز للأطراف اختيار القانون الواجب التطبيق على التزاماتهم التعاقدية. في حال غياب الاختيار، يُطبّق القانون الأكثر صلة بالعقد، مثل مكان إبرامه أو تنفيذه. مع ذلك، لا يُعتد باختيار القانون إذا خالف النظام العام المصري، كأن يسمح بخرق لحقوق المستهلك أو الإفراط في استخدام البيانات.

ووفقًا للمادة ١٨ من القانون المدني، يُسمح للعقد بتحديد القانون المطبق صراحة، ويُقبل هذا الاختيار من قبل المحاكم المصرية إذا كان واضحًا وغير مخالف للنظام العام. وفي عقود السحابة، غالبًا ما يُحدد القانون المصري للعقود المحلية، أو قانون الدولة الأجنبية إذا كان المزود أجنبيًّا، مع الالتزام بحماية البيانات المصرية. ويُطبق القانون الأقرب ارتباطًا (مثل قانون الدولة التي يقع فيها التنفيذ الرئيس أو مقر المزود)، وفقاً لمبادئ القانون الدولي الخاص المصري، حيث يُفضل القانون المصري للنزاعات الوطنية.

أصدر الجهاز القومي لتنظيم الاتصالات إطارًا تنظيميًّا لإنشاء وتشغيل مراكز البيانات وتقديم خدمات الاستضافة والحوسبة السحابية. هذا الإطار يفرض متطلبات وشروطًا على مقدمي الخدمة، ويمكن أن تكون له أهمية في تحديد التزامات الأطراف.

٢- **في القانون الكويتي**: تبنى المشرّع الكويتي نهجًا مشابهًا للمشرع المصري، إذ لم يصدر تنظيم خاص بالتخزين السحابي، وتُطبّق القواعد العامة المنصوص عليها في المواد (٢٧) و(٢٨) من القانون المدني الكويتي، التي تجيز صراحةً للأطراف الاتفاق على القانون الواجب التطبيق في العقود ذات العنصر الأجنبي.

فإذا لم يوجد اتفاق صريح، فإن القانون الكويتي يطبّق قانون الدولة التي تم فيها العقد، أو القانون الذي يُعد أكثر ارتباطًا به بالنظر إلى مكان تنفيذ الالتزامات الجوهرية أو مقر النشاط الرئيس لمقدم الخدمة.

ويلاحظ أن القضاء الكويتي "في قضايا العقود الدولية الإلكترونية" يميل إلى إعمال مبدأ المرونة في الإسناد، بحيث يُعطى الاعتبار لمكان التنفيذ أو لمكان إقامة مقدم الخدمة الرقمية، أكثر من مكان إبرام العقد.

ويمنح القانون الكويتي (وفقًا للمادة ٢٩ من القانون المدني الكويتي) الأطراف حرية اختيار القانون المنظم للعقد. يُشترط أن يكون القانون المختار مرتبطًا بالعقد بشكل معقول. يُستبعد تطبيق أي قانون أجنبي إذا تضمن أحكامًا تتعارض مع النظام العام الكويتي أو الشريعة الإسلامية.

وفي حال عدم وجود اتفاق، يتم الرجوع إلى القانون رقم ٥ لسنة ١٩٦١ بشأن تنظيم العلاقات القانونية ذات العنصر الأجنبي. يحدد هذا القانون القواعد العامة لتنازع القوانين، إذ يسري على الالتزامات التعاقدية، من حيث شروطها الموضوعية وآثارها، قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين إذا اتحدا موطنًا، فإن اختلفا موطنًا يسري قانون الدولة التي تم فيها إبرام العقد. هذا ما لم يتفق المتعاقدان أو يتبين من الظروف أن قانونًا آخر هو الذي يراد تطبيقه.

كما أن القانون رقم ٦٣ لسنة ٢٠١٥ بشأن مكافحة جرائم تقنية المعلومات يفرض عقوبات على الوصول غير المشروع للبيانات أو المعلومات الشخصية أو الحكومية، ويمكن أن يكون له دور في النزاعات التي تتضمن خروقات أمنية.

٣- **القانون الأوروبي (لائحة روما I)**: تنص لائحة روما I (Regulation 593/2008) على أن للأطراف حرية اختيار القانون المنطبق على العقد. في غياب اتفاق، يُطبّق قانون مكان الإقامة الاعتيادي لمقدم الخدمة. تُمنع القواعد المختارة من مخالفة النظام العام الأوروبي أو "قواعد الشرطة" (Lois de police)، كقواعد حماية البيانات[١].

ويمكن القول إن القانون الواجب التطبيق على نزاعات التخزين السحابي لا يزال يُطرح بوصفه أحد الإشكاليات الجوهرية في البيئة القانونية الرقمية، خاصة في ظل غياب تنظيم تشريعي خاص في الدول العربية ومنها مصر والكويت.

حالات قضائية بارزة في النزاعات السحابية:

لقد رسخت الخدمات السحابية مكانتها بوصفها عنصرا لا غنى عنه في البنية التحتية الرقمية العالمية، مقدمةً حلولًا مرنة للشركات والأفراد. ومع هذا التوسع، تتصاعد أيضًا النزاعات القانونية

---

(١) لجنة الأمم المتحدة للقانون التجاري الدولي (الدورة الثالثة والخمسون). (٢٠٢٠). الدليل القانوني إلى الصكوك القانونية الموحدة في مجال العقود التجارية الدولية (مع التركيز على البيع) – مذكرة من الأمانة. ص ٩. ومتاح من خلال الرابط التالي: https://documents.un.org/doc/undoc/gen/v20/011/76/pdf/v2001176.pdf. وتم الاطلاع عليه بتاريخ: ٦/ ٧/ ٢٠٢٥.

التي تكشف عن تعقيدات البيئة السحابية وتحدياتها الفريدة. تُقدم الحالات القضائية البارزة دروسًا قيمة حول مسؤولية مزودي الخدمة، وحماية البيانات، والملكية الفكرية، وصلاحيات الوصول الحكومي في هذا الفضاء الرقمي. وتبين التنوع سواء في طرق حل النزاعات أو القانون المستخدم أما جهة فض النزاع، وفيما يلي بيان لبعض النزاعات مع بيان لكيفية حلها:

١- نزاعات خروقات البيانات ومسؤولية المزود والعميل:

تُعد خروقات البيانات من أبرز أسباب النزاعات في البيئة السحابية، إذ تُثير تساؤلات حول من يتحمل المسؤولية في حال تسرب المعلومات الحساسة.

أ- قضية Capital One Data Breach (2019) [1]:

-**الخلفية**: تعرضت شركة الخدمات المالية العملاقة Capital One لاختراق بيانات ضخمة أثرت على أكثر من ١٠٠ مليون عميل في الولايات المتحدة وكندا. تمكنت مهاجمة من الوصول إلى خادم سحابي تابع لـ Amazon Web Services (AWS) بسبب خطأ في التكوين (misconfiguration) من جانب Capital One.

-**النزاع القانوني والنتائج**: أسفر الاختراق عن سلسلة من الدعاوى القضائية الجماعية ضد Capital One، بالإضافة إلى تحقيقات من قبل الجهات التنظيمية. ركزت الدعاوى على إهمال Capital One في حماية بيانات العملاء. بينما لم تُتهم AWS بشكل مباشر بالخطأ، أكدت القضية على مبدأ المسؤولية المشتركة في السحابة (Shared Responsibility Model)، إذ تقع مسؤولية تأمين البنية التحتية على عاتق مزود السحابة (AWS في هذه الحالة)، بينما تقع مسؤولية أمان البيانات داخل تلك البنية التحتية (مثل التكوينات الصحيحة والتحكم في الوصول) على عاتق العميل (Capital One). في عام ٢٠٢١، وافقت Capital One على دفع ١٩٠ مليون دولار لتسوية الدعاوى القضائية الجماعية.

-**الدرس المستفاد**: تُبرز هذه القضية أهمية فهم وتطبيق نموذج المسؤولية المشتركة في السحابة. لا يُعفي استخدام السحابة العميل من مسؤولية تأمين بياناته. يجب على الشركات التأكد

(1) Khan S., Kabanov I., Hua Y. & Madnick S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. ACM Transactions on Privacy and Security. Vol 26. Iss 1. PP 1–29. https://doi.org/10.1145/3546068.

من أن لديها الإعدادات الأمنية الصحيحة والسياسات المناسبة، وأنها تُجري عمليات تدقيق منتظمة.

ب- قضية Uber Data Breach (2016) وOkta (2022)[1]:

-**الخلفية**: تعرضت شركة أوبر لاختراق كبير في عام ٢٠١٦ أثر على بيانات ٥٧ مليون عميل وسائق. قامت الشركة بإخفاء الاختراق ودفعت للمخترقين لإتلاف البيانات المسروقة بدلًا من الإبلاغ عنها. في قضية Okta، تعرض مزود خدمات إدارة الهوية والوصول لاختراق في عام ٢٠٢٢، مما أثر على العديد من عملائه.

-**النزاع القانوني والنتائج**: في قضية أوبر، أدت فضيحة الإخفاء إلى تحقيق واسع النطاق من قبل السلطات الأمريكية، وغرامات كبيرة (منها ١٤٨ مليون دولار لتسوية مع ٥٠ ولاية أمريكية ومقاطعة كولومبيا). لم تكن المشكلة في فشل مزود الخدمة السحابية بالضرورة، بل في تعامل أوبر مع الاختراق وإخفاقها في الإبلاغ عنه. في قضية Okta، على الرغم من أن الاختراق لم يكن مباشرًا لنظامها الأساس، بل استهدافًا لمقاول خارجي، إلا أنه أثار تساؤلات حول الأمن في سلسلة التوريد السحابية.

-**الدرس المستفاد**: التأكيد على أهمية الشفافية والإبلاغ الفوري عن خروقات البيانات، والمسؤولية القانونية عن إخفاء المعلومات. كما تُسلط الضوء على تحديات الأمن في بيئة السحابة المتسلسلة (supply chain security).

٢- نزاعات الولاية القضائية والوصول الحكومي للبيانات:

تُعدّ صلاحية الدول في الوصول إلى البيانات المخزنة في السحابة، خاصة عندما تكون الخوادم في ولايات قضائية مختلفة، من أكثر القضايا تعقيدًا.

أ- قضية Microsoft Ireland (الولايات المتحدة ضد مايكروسوفت، ٢٠١٨)[2]:

-**الخلفية**: في عام ٢٠١٣، أصدرت محكمة أمريكية أمر تفتيش (warrant) لشركة مايكروسوفت لتقديم رسائل بريد إلكتروني لعميل مشتبه به في قضية مخدرات، وكانت هذه

(1) Choi Y. B. (2021). Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases. International Journal of Cyber Research and Education (IJCRE). Vol 3. Is 1. PP 58-64. https://doi.org/10.4018/IJCRE.2021010106.

(2) Jennifer Daskal. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online. Vol 71. Available through the following link: https://tinyurl.com/26bue4mo. It was viewed on: 28/5/2025.

الرسائل مخزنة على خوادم مايكروسوفت في دبلن، أيرلندا. رفضت مايكروسوفت الامتثال، مجادلة بأن السلطات الأمريكية لا تملك صلاحية قانونية للوصول إلى بيانات مخزنة خارج أراضي الولايات المتحدة.

-**النزاع القانوني والنتائج**: مرت القضية بسلسلة من الاستئنافات ووصلت إلى المحكمة العليا الأمريكية. قبل أن تُصدر المحكمة العليا حكمًا، قام الكونجرس الأمريكي بسن قانون CLOUD Act (Clarifying Lawful Overseas Use of Data Act) في عام ٢٠١٨. هذا القانون يُمكّن السلطات الأمريكية من إجبار شركات التكنولوجيا الأمريكية على تسليم البيانات التي تخُزنها، بغض النظر عن موقعها الجغرافي، مع بعض الآليات للتعاون الدولي. هذا أدى إلى إلغاء القضية (moot).

-**الدرس المستفاد**: تُعد هذه القضية علامة فارقة في النقاش حول سيادة البيانات والولاية القضائية. لقد أبرزت بشكل حاد تضارب القوانين بين الدول في العصر الرقمي، ودفعت نحو تطوير تشريعات وطنية (مثل CLOUD Act) واتفاقيات دولية لتسهيل تبادل البيانات لأغراض إنفاذ القانون، مع الحفاظ على حقوق الخصوصية والسيادة الوطنية.

٣- نزاعات الملكية الفكرية في السحابة:

تُثير الحوسبة السحابية تحديات جديدة بشأن حقوق الملكية الفكرية، سواء للمحتوى المخزن أو للتقنيات المستخدمة.

أ- قضايا براءات الاختراع بين عمالقة التكنولوجيا (مثل Microsoft vs. Salesforce.com)[1]:

-**الخلفية**: في عام ٢٠١١، رفعت مايكروسوفت دعوى قضائية ضد Salesforce.com تتهمها بانتهاك عدة براءات اختراع متعلقة بتقنيات الحوسبة السحابية.

-**النزاع القانوني والنتائج**: تم تسوية هذه القضية خارج المحكمة، مما يُشير إلى تعقيدات النزاعات المتعلقة ببراءات الاختراع في هذا المجال سريع التطور.

---

(1) Chakraborty A. (2014). The Conflicting Economic Views Emerging from the Microsoft Antitrust Case: Literature Review. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2373708.

-**الدرس المستفاد**: تُظهر هذه النزاعات أن سوق الخدمات السحابية، على الرغم من كونه تعاونيًّا في جوانب، فإنه ساحة تنافسية شرسة فيما يتعلق بالملكية الفكرية. يجب على الشركات التي تُطور أو تَستخدم تقنيات سحابية أن تجُري "العناية الواجبة" لضمان عدم انتهاك براءات اختراع قائمة، وأن تحُصّن براءاتها الخاصة.

ب- نزاعات حقوق النشر المتعلقة بالمحتوى المخزن:

-**الخلفية**: على الرغم من أن معظم القضايا البارزة في هذا المجال تتعلق بمنصات التواصل الاجتماعي أو الاستضافة التقليدية، فإن مبادئها تُطبق على الخدمات السحابية. فمثلًا، إذا قام مستخدم بتخزين مواد محمية بحقوق الطبع والنشر (مثل أفلام، موسيقى، برمجيات) بشكل غير قانوني على خدمة تخزين سحابي، فإن مزود الخدمة قد يواجه دعاوى قضائية من أصحاب الحقوق[1].

-**النزاع القانوني والنتائج**: تعتمد المسؤولية القانونية لمزود الخدمة على ما إذا كان يُعد "ناقلًا" (conduit) بريئًا للمحتوى أو "مُضيفًا" (host) مسؤولًا. في العديد من الولايات القضائية، تُقدم القوانين (مثل Digital Millennium Copyright Act - DMCA في الولايات المتحدة) حماية لمزودي الخدمات إذا التزموا بإجراءات "الإشعار والإزالة" (notice and takedown) فور علمهم بالانتهاك[2].

-**الدرس المستفاد**: يجب على مزودي الخدمات السحابية وضع سياسات واضحة لمكافحة انتهاكات حقوق النشر، وتوفير آليات لأصحاب الحقوق للإبلاغ عن المحتوى المخالف، والالتزام بالإجراءات القانونية لإزالة هذا المحتوى.

٤- نزاعات عقود مستوى الخدمة (SLAs) وأداء الخدمة:

تُعد عقود مستوى الخدمة (Service Level Agreements - SLAs) حجر الزاوية في العلاقات السحابية، وتحديد الالتزامات والأداء المتوقع.

---

(1) Валентина Троцька. (2022). ПОЗАСУДОВЕ ВРЕГУЛЮВАННЯ СПОРІВ ЗГІДНО З ЄВРОПЕЙСЬКИМ ЗАКОНОДАВСТВОМ ПРО АВТОРСЬКЕ ПРАВО І СУМІЖНІ ПРАВА В ЄДИНОМУ ЦИФРОВОМУ РИНКУ. Теорія і практика інтелектуальної власності. No 1. PP 35–43. https://doi.org/10.33731/12022.258189.

(2) Zuo X. & Ding H. (2020). Research on Digital Copyright Infringement Based on Cloud Computing Environment. Op. cit. P e012078.

أـ قضية Rackspace vs. Texas (2019)[1]:

-**الخلفية**: رفعت ولاية تكساس دعوى قضائية ضد مزود خدمة سحابية كبير، Rackspace، بسبب انقطاع واسع النطاق للخدمة أثر على العديد من الوكالات الحكومية في الولاية، مما أدى إلى تعطيل العمليات الحيوية.

-**النزاع القانوني والنتائج**: ركزت الدعوى على خرق Rackspace لعقد مستوى الخدمة (SLA) الذي وعد بالحد الأدنى من وقت التشغيل (uptime) والتعافي من الكوارث. تم تسوية القضية خارج المحكمة.

-**الدرس المستفاد**: تُبرز هذه القضية الأهمية القصوى لعقود مستوى الخدمة المحددة بدقة. يجب على العملاء والمزودين فهم التزاماتهم بوضوح، بما في ذلك التعويضات المتوقعة في حال خرق SLA. كما تُشير إلى أن الخسائر الناتجة عن تعطل الخدمات الحكومية أو الحيوية يمكن أن تكون هائلة، مما يستدعي ضمانات قوية في العقود.

بـ نزاعات "خسارة البيانات" الناتجة عن فشل النسخ الاحتياطي أو التعافي:

-**الخلفية**: بينما لا توجد قضية "بارزة" واحدة تُحدد هذا النوع من النزاعات بشكل منفصل، فإن العديد من النزاعات الصغيرة أو التسويات خارج المحكمة تحدث عندما تُفقد بيانات العميل بسبب فشل مزود الخدمة في تنفيذ إجراءات النسخ الاحتياطي أو التعافي من الكوارث المتفق عليها في عقد الـ SLA.

فنزاعات فقدان البيانات الناتجة عن عمليات النسخ الاحتياطي أو الاسترداد الفاشلة من المشكلات الحرجة في إدارة البيانات، خاصة في الأنظمة الموزعة والبيئات السحابية. يمكن أن تؤدي إلى اضطرابات تشغيلية وخسائر مالية وتناقص الثقة في سلامة البيانات. تشمل الاستراتيجيات الفعالة لتقليل فقدان البيانات أنظمة النسخ الاحتياطي القوية وإدارة الاسترداد الفعالة وتنفيذ أفضل الممارسات المصممة خصيصًا لبيئات محددة. توضح الأقسام التالية الجوانب الرئيسة لمعالجة نزاعات فقدان البيانات[2].

(1) Eldar O. & Rauterberg G. V. (2022). Is Corporate Law Nonpartisan? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4125863.

(2) Varun Garg. (2024). Overcoming Data Loss Challenges: Best Practices for Backfill and Reprocessing in Distributed Data Systems. International Journal For Multidisciplinary Research. Vol 6. Is 5. https://doi.org/10.36948/ijfmr.2024.v06i05.21547.

-**النزاع القانوني والنتائج**: تُركز الدعاوى غالبًا على مدى مسؤولية المزود عن فقدان البيانات، ومدى كفاية بنود تحديد المسؤولية والتعويض في العقد.

-**الدرس المستفاد**: يجب أن تُحدد عقود الـ SLA بوضوح سياسات النسخ الاحتياطي، وفترات الاستبقاء، وأوقات التعافي (RTO/RPO)، والتعويضات في حالة فقدان البيانات. يجب على العميل أيضًا أن يكون لديه خطة نسخ احتياطي خارجية مستقلة بوصفها إجراءً احتياطيًّا.

تُقدم الحالات القضائية في مجال الخدمات السحابية لمحة عن المشهد القانوني المتطور لهذه التقنيات. بينما لا تزال العديد من القضايا في طور التسوية أو تُحل خارج المحاكم بسبب تعقيداتها التقنية والقانونية، فإن الأمثلة السابقة تُسلط الضوء على ضرورة صياغة عقود خدمات سحابية شاملة وواضحة تُحدد المسؤوليات والالتزامات بدقة، خاصة فيما يتعلق بالأمن، الخصوصية، الملكية الفكرية، وأداء الخدمة. مع الالتزام بالتشريعات المحلية والدولية لحماية البيانات والخصوصية، خاصة مع تزايد نطاق تطبيقها عبر الحدود[1].

كما أن فهم أن استخدام السحابة لا يُلغي مسؤولية العميل عن تأمين بياناته وتكوين أنظمته بشكل صحيح. وضرورة الإبلاغ الفوري عن خروقات البيانات والتعاون مع الجهات التنظيمية والقضائية. ومع استمرار نمو الاعتماد على الخدمات السحابية، من المتوقع أن تزداد النزاعات القانونية تعقيدًا، مما يستدعي من المحامين، والقضاة، والمشرعين، والمهنيين تقنيين العمل معًا لتطوير أطر قانونية أكثر فعالية وملاءمة للواقع الرقمي المتغير.

(1) J. B K & T. J. (2022). Data Storage Security and Privacy in Cloud Computing. 2022 IEEE International Conference for Women in Innovation. Op. cit. PP 1-10.

المطلب الثاني
طرق فض النزاعات المتعلقة بالحوسبة السحابية

إن احتمالية نشوء النزاعات بين أطراف العلاقة السحابية، سواء بين مزود الخدمة والعميل، أو بين عدة مزودين، أو حتى بين العملاء أنفسهم قائمة بشكل كبير. نظرًا للطبيعة العابرة للحدود، والتقنية المعقدة، والمسؤوليات المتشابكة في البيئة السحابية، وطرق فض النزاعات التقليدية قد لا تكون دائمًا الأكثر كفاءة أو فعالية. لذا، يتطلب الأمر استكشاف آليات مصممة خصيصًا للتعامل مع هذه التحديات الفريدة.

كما يتضح مما سبق أن النزاعات القانونية الناشئة عن خدمات التخزين السحابي تتميز بخصوصية تقنية وتشريعية واضحة. ويعود السبب في ذلك إلى الطبيعة التقنية المعقدة لهذه الخدمات، فضلًا عن التفاوت في الخبرات بين أطراف العلاقة التعاقدية، إذ يتمتع مزودو الخدمات بقدرات تقنية وقانونية متقدمة مقارنة بالعملاء.

فغالبًا ما يقوم مزودو خدمات التخزين السحابي بصياغة العقود في صورة عقود إذعان، وهي تلك العقود التي يفرض فيها طرفٌ شروطه دون منح الطرف الآخر فرصة حقيقية للتفاوض. يظهر ذلك بوضوح في نماذج الاشتراكات الجاهزة أو اتفاقيات المستخدم التي تعرضها الشركات التقنية، مثل اتفاقيات خدمات Google Drive أو Microsoft OneDrive، إذ يتم إعداد الشروط مسبقًا من قبل المزود، وتُعرض على العملاء بوصفها شرطًا أساسيًّا للانتفاع بالخدمة[1].

وبسبب الطبيعة القائمة على عقود الإذعان، يجد العملاء أنفسهم في كثير من الأحيان مضطرين للجوء إلى القضاء التقليدي لحل النزاعات التي تنشأ عن العقود السحابية. وتُعزى هذه الظاهرة إلى أن مزودي الخدمة غالبًا ما يتمتعون بخبرات تقنية وقانونية متقدمة، تجعلهم في موضع قوة عند التفاوض أو إدارة النزاعات، مما يجعل من الصعب على العملاء، وخاصة الأفراد أو المؤسسات الصغيرة، الحصول على حقوقهم بطرق بديلة كالتفاوض أو الوساطة.

المحاكم المختصة بنزاعات التخزين السحابي:

أحدثت خدمات التخزين السحابي تحولًا جوهريًّا في طرق إدارة البيانات وتخزينها عبر الإنترنت، وقد أدى هذا التحول إلى نشوء نزاعات قانونية معقدة ترتبط بعدة أنظمة قانونية وطنية

(1) M. Barati & O. Rana. (2022). Tracking GDPR Compliance in Cloud-Based Service Delivery. in IEEE Transactions on Services Computing. Vol 15. Is 3. PP 1498-1511. doi: 10.1109/TSC.2020.2999559.

ودولية. يعود ذلك إلى الطبيعة العابرة للحدود لعقود الحوسبة السحابية، التي تشمل أطرافًا موزعة جغرافيًّا، وخوادم تقع في دول مختلفة، وعقود تبرم إلكترونيًّا دون حضور مادي.

١- **في القانون المصري**: يُبنى الاختصاص الداخلي للمحاكم المصرية على عدة معايير تهدف إلى توزيع القضايا بين المحاكم المختلفة داخل الدولة بشكل يضمن سير العدالة وتيسير التقاضي على أطراف النزاع. ينقسم هذا الاختصاص بشكل أساس إلى ثلاثة أنواع، الاختصاص القيمي، والاختصاص النوعي، والاختصاص المحلي[(١)].

تنص المادة (٢٨) من قانون المرافعات على أن الاختصاص ينعقد للمحكمة التي يقع في دائرتها موطن المدعى عليه، أو التي تم فيها تنفيذ الالتزام. لكن في عقود الحوسبة السحابية، قد لا يوجد مقر مادي للمدعى عليه في مصر، مما يُعقد مسألة الاختصاص.

---

(١) **الاختصاص المحلي (المكاني)**: هذا هو المبدأ الأساس الذي يحدد المحكمة المختصة جغرافيًّا بنظر الدعوى. القاعدة العامة في هذا الشأن نصت عليها المادة ٤٩ من قانون المرافعات، التي تعد حجر الزاوية في تحديد الاختصاص المحلي.

فالقاعدة العامة؛ محكمة موطن المدعى عليه (المادة ٤٩)، "يكون الاختصاص للمحكمة التي يقع في دائرتها موطن المدعى عليه ما لم ينص القانون على خلاف ذلك". فالأصل أن المدعي هو الذي يسعى إلى خصمه في محكمته. لذلك، يجب رفع الدعوى أمام المحكمة التي يقع في نطاقها الجغرافي موطن الشخص المطلوب مقاضاته (المدعى عليه).

الموطن هو المكان الذي يقيم فيه الشخص عادةً (وفقًا للقانون المدني). بالنسبة للشركات والأشخاص الاعتبارية، يكون موطنها هو المكان الذي يوجد فيه مركز إدارتها الرئيس.

الاختصاص القيمي والنوعي (المواد ٤١ – ٤٨): هذه المعايير تحدد نوع المحكمة (جزئية أم ابتدائية) ودرجتها التي ستنظر النزاع بناءً على قيمة الدعوى أو طبيعتها.

الاختصاص القيمي للمحاكم الجزئية (المادة ٤٢)، إذ تختص المحكمة الجزئية بالحكم ابتدائيًّا في الدعاوى التي لا تتجاوز قيمتها مائتي ألف جنيه. ويكون حكمها نهائيًّا إذا كانت قيمة الدعوى لا تتجاوز ثلاثين ألف جنيه. (تم تعديل هذه القيم بالقانون رقم ١٩١ لسنة ٢٠٢٠). والاختصاص النوعي للمحاكم الجزئية (المادة ٤٣)، تختص المحكمة الجزئية بنوع معين من الدعاوى بغض النظر عن قيمتها، مثل دعاوى قسمة المال الشائع ودعاوى فرز وتجنيب الحصة. الاختصاص العام للمحاكم الابتدائية (المادة ٤٧) تختص المحاكم الابتدائية بنظر كافة الدعاوى التي ليست من اختصاص المحاكم الجزئية (أي التي تزيد قيمتها على مائتي ألف جنيه). كما تختص بنظر الدعاوى المتعلقة بالجنسية وشهر الإفلاس والصلح الواقي منه.

إذا كان أحد الأطراف مصريًا، وكانت الخدمة موجهة إلى السوق المصري، قد تستند المحكمة إلى فكرة "الاختصاص القضائي المستمد من الضرر أو التنفيذ". وجود شرط اختصاص قضائي في العقد يُعتد به إذا لم يتعارض مع النظام العام.

كما ميّز بين الاختصاص الداخلي الذي يتعلق بتوزيع القضايا بين المحاكم داخل الدولة، والاختصاص الدولي الذي يحدد متى تكون المحاكم المصرية مختصة بنظر المنازعات ذات العنصر الأجنبي.

ويركّز هذا الجزء على الاختصاص الداخلي، الذي يخضع أساسًا للأحكام الواردة في المواد من (٢٨) إلى (٦٣) من قانون المرافعات المصري، الذي يحدد المعايير القانونية لتوزيع الدعاوى بين المحاكم المختلفة بحسب نوعها أو قيمتها أو مكانها الجغرافي.

وعند بحث النزاعات الناشئة عن عقود التخزين السحابي داخل مصر، يجب أولًا؛ التحقق مما إذا كان النزاع داخليًا بحتًا أم ذا طابع دولي. فإذا كان النزاع بين طرفين داخل الإقليم المصري، تُطبَّق القواعد العامة للاختصاص المنصوص عليها في المادة (٢٨) وما بعدها. إذا كان مقر شركة التخزين السحابي في القاهرة، والمستخدم يقيم في الإسكندرية، فينعقد الاختصاص لمحكمة موطن المدعى عليه (شركة التخزين) ما لم يُتفق على خلاف ذلك في العقد الإلكتروني.

أما إذا كان أحد الأطراف أجنبيًا أو الخدمة مقدمة من خوادم خارج الإقليم المصري، ينتقل النقاش إلى الاختصاص الدولي وتحديد القانون الواجب التطبيق (Lex Causae).

إن المادة (٢٨) وما بعدها من قانون المرافعات تمثل الإطار الحاكم للاختصاص الداخلي في النظام القضائي المصري، وهي تُرسخ مبدأ الموازنة بين حقوق الخصوم في اختيار جهة التقاضي المناسبة، وتضمن استقرار المعاملات القانونية داخل الإقليم المصري.

وبالتالي؛ فإن التفرقة بين الاختصاص الداخلي والدولي تُعدّ نقطة الانطلاق الجوهرية لأي دراسة تتناول النزاعات القانونية المرتبطة بالخدمات الرقمية أو عقود التخزين السحابي، لأنها تحدد الجهة القضائية المختصة، ومن ثم القانون الواجب التطبيق والآثار القانونية المترتبة على النزاع.

٢ـ **في القانون الكويتي**: نصوص قانون المرافعات الكويتي تُشابه إلى حد كبير ما ورد في القانون المصري، إذ يُعتد بمكان إقامة المدعى عليه أو مكان تنفيذ الالتزام. يُلاحظ أن القضاء الكويتي يعطي أهمية للاتفاقات المسبقة في العقود الإلكترونية، بشرط عدم الإضرار بالطرف الأضعف (المستهلك). وفي غياب اتفاق صريح، قد تعتمد المحاكم على معيار "صلة النزاع بالواقع المحلي".

وعندما يتعلق النزاع بعلاقة قانونية تشتمل على عنصر أجنبي (كأن يكون أحد الأطراف أجنبيًّا، أو أن العقد تم إبرامه أو سيُنفذ في الخارج)، فإننا نخرج من نطاق الاختصاص الداخلي وندخل في إطار القانون الدولي الخاص. ينظم المشرع الكويتي هذه المسائل في قانونين رئيسين؛ قانون تنظيم العلاقات القانونية ذات العنصر الأجنبي (القانون رقم ٥ لسنة ١٩٦١) وهو القانون الذي يحدد "القانون الواجب التطبيق" (Lex Causae) على النزاع. وقانون المرافعات المدنية والتجارية (المرسوم بالقانون رقم ٣٨ لسنة ١٩٨٠) وهو القانون الذي يحدد "المحكمة المختصة" بنظر النزاع.

فالقانون الواجب التطبيق (Lex Causae) في ضوء القانون رقم ٥ لسنة ١٩٦١ يضع قواعد الإسناد التي ترشد إلى القانون الذي يجب عليه تطبيقه على النزاع الدولي. المبدأ الأساس في العقود الدولية هو سلطان الإرادة، ولكن في غيابه، يضع القانون حلولاً بديلة.

فالمادة (٦٩) من القانون رقم ٥ لسنة ١٩٦١ تنص على؛ "يسري على الالتزامات التعاقدية، من حيث شروطها الموضوعية وآثارها، قانون الدولة التي يوجد فيها الموطن المشترك للمتعاقدين إذا اتحدا موطنا، فإن اختلفا موطنا يسري قانون الدولة التي تم فيها إبرام العقد. هذا ما لم يتفق المتعاقدان أو يتبين من الظروف أن قانونا آخر هو الذي يراد تطبيقه".

الجزء الأخير من المادة هو الأهم في العقود الدولية. فهو يعطي الأطراف الحرية الكاملة في اختيار القانون الذي سيحكم عقدهم صراحةً أو ضمنًا.

ومعظم عقود الخدمات السحابية التي تقدمها الشركات العالمية (مثل Amazon Web Services, Microsoft Azure, Google Cloud) تتضمن بندًا صريحًا يحدد القانون الواجب التطبيق (غالبًا قانون ولاية واشنطن أو كاليفورنيا في الولايات المتحدة أو قانون أيرلندا في أوروبا). إذا عرض نزاع متعلق بهذه العقود على قاضٍ كويتي، فإنه سيطبق القانون الذي اختاره الأطراف.

إذا لم يتفق الأطراف صراحة أو ضمنًا على قانون معين، فإن المادة (٦٩) نفسها تضع قواعد إسناد احتياطية:

-**قانون الموطن المشترك**: إذا كان للمتعاقدين موطن مشترك في دولة واحدة، يسري قانون هذه الدولة.

-**قانون محل إبرام العقد**: إذا اختلف موطنهما، يسري قانون الدولة التي أُبرم فيها العقد. في سياق العقود الإلكترونية مثل التخزين السحابي، يمكن أن يثير تحديد "مكان إبرام العقد"

صعوبات، ولكن غالبًا ما يعتبر هو المكان الذي صدر فيه القبول (أي مكان وجود خوادم مقدم الخدمة أو مركز إدارته).

فحرية الأطراف ليست مطلقة، بل ترد عليها قيود تهدف لحماية المصالح العليا للدولة، وأهمها؛ النظام العام والآداب (المادة ٨٠) لا يجوز تطبيق أحكام قانون أجنبي تم اختياره إذا كانت هذه الأحكام تخالف النظام العام أو الآداب في دولة الكويت. على سبيل المثال، إذا كان القانون الأجنبي يسمح بفوائد فاحشة تعتبرها المحاكم الكويتية استغلالًا، فقد تستبعد هذا الحكم. والقواعد الآمرة هناك قوانين كويتية تطبق مباشرة على أي علاقة تعرض على القاضي الكويتي بغض النظر عن القانون المتفق عليه، لأنها تتعلق بسيادة الدولة ومصالحها الأساسية. ومن أبرز الأمثلة؛ الإطار التنظيمي للحوسبة السحابية (قرار CITRA رقم ١١٢ لسنة ٢٠٢١) الذي يفرض التزامات مباشرة على مقدمي الخدمة، مثل حظر تخزين البيانات الحكومية الحساسة خارج الكويت. هذه قاعدة آمرة لا يمكن الاتفاق على مخالفتها، وستطبقها المحكمة الكويتية مباشرة، حتى لو كان العقد يخضع لقانون أجنبي.

وقانون حماية البيانات الشخصية (القانون رقم ٢٠ لسنة ٢٠٢٤) الذي يفرض التزامات تتعلق بمعالجة البيانات الشخصية داخل الكويت، وتعتبر أحكامه من النظام العام.

٣- **في القانون الأوروبي (نظام بروكسل)**: تُعتمد قواعد لائحة بروكسل (Regulation 1215/2012) لتحديد الاختصاص في الاتحاد الأوروبي[1]:

- الأصل أن الاختصاص ينعقد لمحاكم الدولة التي يقع فيها موطن المدعى عليه.
- في عقود الخدمات، ينعقد الاختصاص لمحكمة مكان تقديم الخدمة أو مكان التنفيذ الرئيس للعقد.
- يُعترف باتفاقات الاختصاص القضائي المسبقة ما دامت واضحة وغير تعسفية.

(1) Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Available through the following link: https://eur-lex.europa.eu/eli/reg/2012/1215/oj/eng. It was viewed on: 6/7/2025.

إن اختلاف النُظم القضائية، يجعل من تحديد المحكمة المختصة والقانون على نزاعات التخزين السحابي مسألة معقدة، تتطلب مراجعة تشريعية دقيقة، وتأطيرًا قانونيًّا جديدًا ينسجم مع الواقع الرقمي المتغير.

طرق فض النزاعات التقليدية في سياق الحوسبة السحابية:

على الرغم من التطور الهائل في طرق فض النزاعات الرقمية، لا تزال الطرق التقليدية "وبخاصة المفاوضات المباشرة والتقاضي أمام المحاكم" تحافظ على مكانة مهمة في التعامل مع النزاعات الناشئة عن عقود وخدمات التخزين السحابي. ومع ذلك، فإن هذه الأساليب تواجه تحديات متعددة تتناسب مع طبيعة السحابة والبيئة التقنية المتطورة[١].

١ـ المفاوضات المباشرة: تُعد المفاوضات المباشرة أول خطوة يلجأ إليها الأطراف المتنازعون. وهي عبارة عن محادثات مباشرة يجريها الأطراف أنفسهم أو ممثلوهم (مثل فرق الدعم الفني أو القانوني لدى مزودي الخدمة). الهدف منها هو التوصل إلى حل ودي دون اللجوء إلى أطراف خارجية أو تدخل طرف ثالث[٢].

أهميتها في بيئة السحابة: في كثير من النزاعات السحابية، تكون المفاوضات المباشرة كافية لحل قضايا صغيرة مثل مشاكل الفوترة أو الاستخدام، خاصة إذا لم يكن هناك ضرر مالي جسيم أو خرق للقانون. وقد يستعين العميل بفريق الدعم الفني لمزود الخدمة لتسوية الأمور. على سبيل المثال، إذا واجه عميل مشكلة في سعة التخزين أو انقطاع الخدمة، يمكن تسويتها عبر التواصل مع مزود الخدمة مباشرة دون حاجة لإجراءات قانونية[٣].

---

(1) Limam S, Belalem G. (2016). A self-adaptive conflict resolution with flexible consistency guarantee in the cloud computing. Multiagent and Grid Systems. Vol 12. Is 3. PP 217-238. doi:10.3233/MGS-160251

(2) Tippavajjula A., Pappachan P., Squicciarini A. & Such J. (2024). ACCORD: Constraint-driven Mediation of Multi-user Conflicts in Cloud Services. In Companion Proceedings of the ACM Web Conference 2024 (pp. 1039–1042). WWW '24: The ACM Web Conference 2024. ACM. https://doi.org/10.1145/3589335.3651244.

(3) Paputungan I. V. (2023). Chapter 17- Explainable renegotiation for SLA in cloud-based system. In Explainable Artificial Intelligence (XAI): Concepts, enabling tools, technologies and applications Institution of Engineering and Technology. PP 329–346. https://doi.org/10.1049/pbpc062e_ch17.

تحديات المفاوضات المباشرة: على الرغم من سهولة هذه الطريقة، فإنها قد تفشل عندما تكون هناك فجوة كبيرة في القوة التفاوضية بين مزودي الخدمة والعملاء. فغالبًا ما يكون لدى مزودي الخدمة مهارات قانونية وتقنية متقدمة، بينما يفتقر العملاء إلى الخبرة اللازمة. كما أن القضايا المعقدة "كالتعدي على حقوق الملكية الفكرية أو انتهاك سرية البيانات" قد تتجاوز قدرة المفاوضات المباشرة على إيجاد حلول فعالة، وتتطلب تدخلًا قضائيًا أو تحكيميًا[١].

٢ـ **التقاضي أمام المحاكم**: يُقصد بالتقاضي عرض النزاع أمام محكمة مختصة وفقًا للقواعد الإجرائية الموضوعية، إذ يصدر القاضي حكمًا ملزمًا للطرفين. ويُعتبر الخيار الأخير في سلسلة فض المنازعات، عندما تفشل جميع محاولات التسوية البديلة.

الملاءمة في البيئة السحابية: يُعد التقاضي مناسبًا في القضايا التي تتضمن خسائر مالية كبيرة، أو انتهاكات لخصوصية البيانات، أو خروقات جسيمة لشروط الاستخدام، أو حالات اختراق البيانات الحساسة. كما يُلجأ إليه عندما تنتهي المهلة القانونية لحل النزاع دون نتائج[٢].

التحديات المرتبطة بالتقاضي في السحابة: نظرًا لأن البيانات السحابية موزعة عبر خوادم متعددة في دول مختلفة، يصبح تحديد الدولة والمحكمة المختصة بنظر النزاع أمرًا معقدًا. قد تُحدد عقود الاستخدام مسبقًا ولاية قضائية معينة (مثل ولاية كاليفورنيا في الولايات المتحدة)، لكنها قد لا تُناسب العميل الموجود في دولة عربية، ما يُثير إشكالات تتعلق بالنفاذ والعدالة[٣].

---

(1) Anithakumari S., Chandrasekaran K. (2017). Negotiation and Monitoring of Service Level Agreements in Cloud Computing Services. In: Satapathy S., Bhateja V., Joshi A. (eds) Proceedings of the International Conference on Data Engineering and Communication Technology. Advances in Intelligent Systems and Computing. Springer, Singapore. Vol 469. https://doi.org/10.1007/978-981-10-1678-3_62.

(2) Meglio M. (2020). Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation. Boston College Law Review. Vol 61. Is 3. PP 1223-1269.

(3) Jarjis Khalaf Saleh F. & Omar Al Amr S. (2023). Conflict of Legislative and Judicial Jurisdiction in Electronic Contract Disputes - A Comparative Study. Alanya International Congress of Social Sciences. Rimar Academy. PP 101–114. https://doi.org/10.47832/alanyacongress2-10.

وحتى مع تحديد المحكمة، يبقى هناك خلاف حول القانون الذي يُطبق: هل هو قانون الدولة التي يوجد بها مقر مزود الخدمة؟ أم قانون الدولة التي يوجد بها العميل؟ أم قانون الدولة التي حدثت فيها المخالفة فعليًّا؟ هذه التعقيدات تجعل النزاع أكثر صعوبة من الناحية القانونية.

كما يتسم التقاضي في أغلب النظم القانونية بطول المدة والإجراءات المعقدة، وهو ما لا يتلاءم مع طبيعة الخدمات السحابية التي تتغير بسرعة، وتُعتمد بشكل يومي في الأعمال. كما أن التكاليف المرتفعة كأتعاب المحامين والرسوم القضائية قد تُثني الأطراف، خاصة الأفراد، عن اللجوء للقضاء.

وأحد أبرز الإشكاليات هو عدم توفر الخبرة الفنية لدى القضاة لفهم تفاصيل دقيقة تتعلق بالبنية التحتية السحابية، مثل التشفير، النسخ الاحتياطي، توزيع البيانات، أو التكوين الأمني. هذا النقص قد يؤدي إلى صدور أحكام غير دقيقة أو غير عادلة من الناحية الفنية. يمكن أن تعوق هذه الفجوة في الفهم قدرتهم على اتخاذ قرارات مستنيرة في القضايا القانونية التي تنطوي على الحوسبة السحابية. توضح الأقسام التالية التحديات والاعتبارات الرئيسة المتعلقة بهذه القضية[1].

يتضح مما سبق أن الطرق التقليدية لفض النزاعات -على الرغم من أهميتها- تواجه تحديات جوهرية في سياق السحابة الإلكترونية. وعلى الرغم من أنها قد تُشكل ضمانة قانونية أقوى للطرف الأضعف في العقد، فإن كفاءتها تتوقف على القدرة على تذليل العقبات القضائية والتشريعية والتقنية المرتبطة بهذه البيئة الرقمية. وهو ما يدفع للاهتمام بدمج الحلول التقليدية مع تقنيات فض النزاعات الحديثة لمواجهة طبيعة النزاعات المستقبلية في الفضاء الرقمي.

محل تنفيذ الالتزام في العقود الإلكترونية والتخزين السحابي:

في العقود التقليدية، تحديد محل التنفيذ أمر واضح ومادي (مكان تسليم البضاعة، أو تسديد الثمن). ولكن في العقود الإلكترونية، وخاصة عقود التخزين السحابي، يصبح محل التنفيذ افتراضيًّا أو غير مادي لأن الخدمة تُقدَّم عبر الإنترنت، والخوادم قد تكون موزعة في دول متعددة. لذلك، يُعتمد على أحد المعايير التالية لتحديد محل التنفيذ:

---

(1) Nanda A. K., Sharma A., Augustine P. J., Cyril B. R., Kiran V., & Sampath B. (2024). Securing Cloud Infrastructure in IaaS and PaaS Environments. In P. Goel, H. Pandey, A. Singhal, & S. Agarwal (Eds.), Improving Security, Privacy, and Trust in Cloud Computing. IGI Global Scientific Publishing. PP 1-33. https://doi.org/10.4018/979-8-3693-1431-9.ch001.

- **محل إقامة مقدم الخدمة (مزود التخزين السحابي)**: بوصفه الطرف الذي يؤدي الالتزام الأساس (توفير الخدمة وتخزين البيانات). وهذا هو الاتجاه الراجح فقهيًّا، باعتبار أن تنفيذ الالتزام الفعلي يتم من خلال البنية التحتية المملوكة له.

- **محل إقامة المستخدم (العميل)**: إذا كان الالتزام محل النزاع يتعلق بالانتفاع بالخدمة أو حماية البيانات الشخصية للمستخدم داخل دولته. وهذا المعيار غالبًا ما يُستخدم لحماية المستهلكين في العقود الإلكترونية الدولية.

- **مكان الخادم (Server Location)**: وهو معيار تقني يُستعان به في بعض القوانين الحديثة لتحديد الاختصاص، على الرغم من أنه عمليًّا غير دقيق لأن الخوادم تكون غالبًا في دول مختلفة ولا تخضع لسيطرة قانونية واحدة.

- **الاتفاق الصريح**: وهو الحل الأمثل، إذ يمكن للأطراف أن ينصوا في العقد الإلكتروني على أن "محل تنفيذ الالتزام" هو مقر الشركة، أو بلد العميل، أو أي مكان آخر يتفقون عليه. وهذا الاتفاق يُعتدّ به قانونًا طالما لا يخالف النظام العام.

فمحل تنفيذ الالتزام المكان الذي يجب على المدين أن يقوم فيه بتنفيذ ما التزم به لصالح الدائن، سواء كان الالتزام بإعطاء شيء، أو بالقيام بعمل، أو بالامتناع عن عمل. ويترتب على تحديد هذا المكان آثار قانونية مهمة، منها؛ تحديد المحكمة المختصة بنظر النزاع (وفقًا لقواعد الاختصاص المحلي والدولي)، وتحديد القانون الواجب التطبيق (عند وجود عنصر أجنبي في العلاقة).

وتنص المادة (٣٤٥) من القانون المدني المصري على أنه؛ "يكون تنفيذ الالتزام في المكان الذي عيّنه الاتفاق أو استخلص من طبيعة الالتزام أو من ظروف الحال". فإذا لم يُحدد مكان تنفيذ الالتزام صراحة، تُطبّق القواعد التالية:

- في الالتزامات بنقل ملكية شيء معين بالذات أو تسليمه، ويكون التنفيذ في المكان الذي يوجد فيه هذا الشيء وقت نشوء الالتزام.

- في الالتزامات بدفع مبلغ من النقود، يكون التنفيذ في موطن الدائن وقت الوفاء.

- في غير ذلك من الالتزامات، يكون التنفيذ في موطن المدين وقت نشوء الالتزام.

وبالتالي، المعيار الأساس هو طبيعة الالتزام ومضمونه.

وفي القانون الكويتي؛ المبدأ ذاته قرره المشرع الكويتي في المادة (٢٠٨) من القانون المدني الكويتي التي تنص على؛ "يُنفّذ الالتزام في المكان الذي عُيِّن أو اتفق عليه، فإذا لم يُعيَّن وجب تنفيذ

الالتزام في موطن المدين وقت نشوئه، ما لم يكن هناك عرف أو طبيعة المعاملة تقتضي غير ذلك". وهذا يعني أن الأصل هو موطن المدين، ما لم يوجد اتفاق أو عرف أو ظروف تدل على خلاف ذلك.

خامسًا: الأثر القانوني لتحديد محل تنفيذ الالتزام

وإذا كانت الخدمة موجهة لمستخدم في الكويت، فيُعتبر الالتزام منفذًا داخل الكويت، وتختص المحاكم الكويتية بالنزاع. ومن حيث تحديد القانون الواجب التطبيق (Lex Loci Solutionis)، تطبّق المحاكم عادةً قانون مكان التنفيذ ما لم يتفق الطرفان على خلاف ذلك. أي أن محل التنفيذ يُستخدم بوصفه ضابط إسناد في تنازع القوانين.

إن محل تنفيذ الالتزام في عقود التخزين السحابي لا يمكن حصره في مكان مادي، بل يجب تحديده وفقًا لمعيار الإرادة المشتركة للأطراف والطبيعة التقنية للالتزام. وبالتالي، إذا لم يُنص عليه صراحة في العقد، يمكن استخلاصه من موطن مقدم الخدمة، ومكان انتفاع المستخدم، أو موقع الخوادم المستخدمة في تقديم الخدمة.

تعدد أماكن الضرر وأثره في تحديد المحكمة المختصة:

عند تعدد أماكن وقوع الضرر، يثور التساؤل حول الدولة المختصة بنظر النزاع. وقد استقر الفقه والقضاء المقارن، خاصةً في النظم الأنجلوسكسونية واللاتينية على أن الاختصاص يمكن أن ينعقد إما لمحكمة مكان حدوث الفعل الضار، أو محكمة مكان تحقق الضرر، وذلك اتساقًا مع مبدأ "الاختصاص الاختياري" في المسؤولية التقصيرية.

ويُستدل في هذا السياق بما قررته محكمة العدل الأوروبية (ECJ) في قضية Mines de Potasse d'Alsace، التي أرست القاعدة القائلة بأن للمضرور الخيار في إقامة الدعوى أمام محكمة مكان الفعل المسبب للضرر أو أمام محكمة مكان تحقق النتيجة الضارة[1].

وبالقياس على ذلك، يمكن القول في النزاعات السحابية إذ ينتج الضرر في أكثر من دولة أن للمضرور أن يلجأ إلى محاكم الدولة التي وقع فيها الأثر الملموس للضرر، شريطة أن تكون لهذه الدولة صلة حقيقية بالنزاع، كوجود مركز أعمال المستخدم أو مقره التقني فيها.

---

(1) Judgment of the Court of 30 November 1976. Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA. Reference for a preliminary ruling: Gerechtshof 's-Gravenhage - Netherlands. Brussels Convention on jurisdiction and the enforcement of Judgment - Article 5 (3) (liability in tort, delict or quasi-delict). Case 21-76. Available through the following link: https://curia.europa.eu/juris/liste.jsf?&num=21/76. It was accessed on 1/10/2025.

أما في القانون المصري، فيُفهم من نصوص المواد ٢٨ و٣٠ من قانون المرافعات المدنية والتجارية أن الاختصاص ينعقد للمحكمة التي وقع في دائرتها الفعل المسبب للضرر أو التي تحقق فيها الضرر فعلًا. وهذا المفهوم يمكن تطبيقه في البيئة الرقمية مع بعض التكييف التقني، إذ قد يُعد "مكان تحقق الضرر" هو الموقع الجغرافي لخوادم التخزين أو مقر المستخدم المتضرر.

وفي القانون الكويتي، يتبنى الاتجاه ذاته من خلال القواعد العامة للاختصاص المكاني في المسؤولية التقصيرية، ويُضاف إليه معيار "أوثق صلة قانونية"، المنصوص عليه في بعض التطبيقات القضائية والمعاهدات الدولية التي صادقت عليها الكويت، بحيث يُرجَّح اختصاص الدولة التي ترتبط بالنزاع بأقوى علاقة واقعية وقانونية.

أما في حالة تعاقب الأضرار وتسلسلها "أي عندما ينشأ ضرر أولي في دولة معينة، ثم تتولد عنه أضرار لاحقة في دول أخرى" فإن الإشكال يصبح أكثر تعقيداً. فكل دولة قد تدّعي اختصاصها القضائي بالنظر إلى الضرر الذي تحقق داخل إقليمها.

وقد عالج الفقه الدولي هذا الإشكال من خلال مبدأ "مركز الثقل للضرر" (Center of Gravity of the Damage)، أي الدولة التي تحقق فيها الضرر الجوهري أو الأساس، وهي التي ينعقد لها الاختصاص القضائي ويُرجَّح تطبيق قانونها بوصفه القانون الأقرب.

وفي ضوء ذلك، فإن القاضي ينبغي أن يميز بين الضرر المباشر والرئيس الذي يمثل جوهر النزاع، وبين الأضرار غير المباشرة أو التبعية التي تقع تباعاً في دول أخرى، ويقصر الاختصاص على محل الضرر الجوهري، منعًا لتعدد الاختصاصات وتضارب الأحكام.

أما في البيئة السحابية، حيث يمكن أن ينتقل الضرر بسرعة بين عدة خوادم ومستخدمين حول العالم، فإن هذا المبدأ يُترجم عمليًّا إلى البحث عن "النقطة القانونية المركزية للضرر"، أي الخادم أو الجهة أو المستخدم الذي انطلقت منه السلوكيات المسببة للضرر. وهذا ما ينبغي أن يكون محور الاختصاص والقانون الواجب التطبيق، تحقيقًا للعدالة وتفاديًا لفوضى التنازع القضائي الدولي.

الوسائل البديلة لفض النزاعات السحابية:

مع التوسع في البيئة الرقمية خاصة في استخدام خدمات التخزين السحابي، تتزايد النزاعات التقنية المرتبطة بهذه البيئة، سواء كانت بين العملاء ومزودي الخدمة أو بين الأطراف ذات العلاقة بالسحابة مثل الشركاء من مزودي البنية التحتية أو العملاء المتعددين. وقد دفعت هذه النزاعات إلى

التفكير جديًّا في سبل فض النزاعات الملائمة، خاصة في ضوء تعقيدات البيئة التقنية وعبر الحدود التي تُصعّب من إجراءات التقاضي التقليدي. هنا، تُطرح بدائل تسوية النزاعات بوصفها خيارا عمليا وعصريا، يُمكنه التكيف مع هذه المتغيرات، بما يوفر مرونة وسرعة وقدرة على استيعاب الطبيعة التقنية الخاصة للنزاعات السحابية[١].

فالوساطة الإلكترونية؛ تُعد وسيلة غير رسمية تُساعد الأطراف المتنازعة على الوصول إلى حل ودي من خلال طرف محايد يُيسر النقاش بينهم. هذه الوسيلة تمتاز بقدرتها على معالجة النزاعات الناشئة عن مشكلات تقنية محدودة، مثل سوء الفوترة أو الأعطال اليسيرة، التي قد لا تتطلب تحكيمًا أو حكمًا قضائيًّا. وقد ساعدت التشريعات الحديثة في بعض الأنظمة القانونية، مثل توجيه الاتحاد الأوروبي رقم ٢٠٠٨/ ٥٢/ EC، في تقنين وتشجيع الوساطة بوصفها خيارا بديلا للنزاعات، بينما في النظم القانونية العربية مثل القانون المصري، لا تزال الوساطة الإلكترونية غير منظمة بشكل خاص، وإن كان هناك اعتراف عام بها في إطار "التسوية الودية" في القوانين المدنية والتجارية. وفي الكويت، تُعتمد الوساطة أداة للصلح القضائي، ولكنها تحتاج مزيدًا من التنظيم لكي تصبح أداة فعالة للتعامل مع النزاعات الرقمية[٢].

والتحكيم الإلكتروني يُعد أحد أبرز الوسائل البديلة التي تتوافق مع طبيعة النزاعات السحابية. يتم من خلاله حل النزاعات بقرارات مُلزمة تصدرها هيئات تحكيمية، ويجري غالبًا عبر منصات إلكترونية تتيح تقديم الأدلة والمستندات رقميًّا. تكمن أهميته في قدرته على استيعاب الجوانب الفنية والتقنية البحتة مثل مستوى التشفير والأمان الرقمي، وبفضل إمكانية اختيار محكّمين خبراء تقنيًّا. وتبرز التحديات في البيئة السحابية مثل صعوبة تحديد القانون الواجب التطبيق أو المحكمة المختصة، وهو ما يُعرف بـ"الاختصاص القضائي" الذي تُثيره الطبيعة العابرة للحدود لعقود

---

(1) Dayanim Behnam & George Edward (2018). Data breach litigation and regulatory enforcement: A survey of our present and how to prepare for the future. In the Cyber Security: A Peer-Reviewed Journal. Vol 1. Is 4. P 301. https://doi.org/10.69554/JJSA8822..

(2) Gavrila S. P. (2024). CHALLENGES AND DIRECTIONS OF THE EUROPEAN REGULATION OF MEDIATION IN CROSS-BORDER DISPUTES. SWS International Scientific Conferences on SOCIAL SCIENCES – ISCSS. Vol 11. PP 115–126. https://doi.org/10.35603/sws.iscss.2024/vs02/04.

السحابة[١]. في مصر، نظم قانون التحكيم رقم ٢٧ لسنة ١٩٩٤ أسس التحكيم التقليدي، وهو يفسح المجال لقبول التحكيم الإلكتروني ضمن أطر مرنة إذا احترم المبادئ الأساسية كالإرادة الحرة للأطراف. أما في الكويت، فلا يوجد نص خاص بالتحكيم الإلكتروني، لكن تظل مبادئ قانون التحكيم رقم ١١ لسنة ١٩٩٥ صالحة للتطبيق على هذا النوع من النزاعات. وفي المقابل، يُشجع الاتحاد الأوروبي بقوة آليات التحكيم الإلكتروني في إطار حماية المستهلك والثقة الرقمية[٢].

ويُشكل لجوء الأطراف إلى "لجان الخبرة التقنية" خيارًا مناسبًا عندما تتعلق النزاعات بمسائل تقنية بحتة يصعب على القضاة أو المحكمين غير المتخصصين فهمها بدقة. مثلًا، عند نشوء نزاع بشأن فشل مزود الخدمة في تطبيق معايير الأمان أو تفسير تفاصيل التشفير أو فقدان البيانات. هنا، تلعب الخبرة التقنية دورًا رئيسًا في توجيه الأطراف إلى تقييم دقيق للوقائع الفنية وتحديد مواضع القصور أو الانتهاك. تتمثل قوة هذه الخبرة في مرونتها وعدم طابعها الملزم "ما لم يتفق الأطراف على إلزامها"، وهو ما يتيح استخدامها بوصفها خطوة استباقية قبل اللجوء إلى القضاء أو التحكيم. يُعد هذا الخيار حلًا عمليًا لتقليص حجم النزاعات التي قد تنشأ لاحقًا أو للتقليل من التكاليف المرتفعة المرتبطة بالتقاضي أمام المحاكم[٣].

وعند مقارنة الأطر القانونية المعنية بهذه الوسائل في القوانين المصرية والكويتية والأوروبية، يظهر تفاوت واضح في مدى التنظيم. ففي مصر، على الرغم من وجود نصوص عامة تنظم الوساطة والتحكيم، فإن الوساطة الإلكترونية والتحكيم الإلكتروني لم يُنظما صراحةً، مما يفتح الباب أمام التكييف القضائي والاتفاقات الخاصة بين الأطراف. وفي الكويت، توجد أحكام عامة للصلح

---

(1) Kheira A. (2024). Electronic Arbitration as an Alternative Mechanism for Resolving E-Commerce Disputes. Journal of Lifestyle and SDGs Review. Vol 4. Is 4. P e04292. https://doi.org/10.47172/2965-730X.SDGsReview.v4.n04.pe04292.

(٢) شرف خالد إبراهيم. (٢٠٢٢). اتفاق التحكيم الدولي المبرم من خلال التطبيقات الإلكترونية: التعليق على قضية "سناب شات" أمام المحاكم الكويتية. جامعة الكويت – مجلس النشر العلمي. مجلد ٤٦. عدد ٤. الصفحات ١١٥ – ١٦٥.

(3) AVSIYEVYCH A. (2024). PROSPECTS OF INFORMATION TECHNOLOGY USE IN INTERNATIONAL COMMERCIAL ARBITRATION DISPUTE RESOLUTION. Naukovyy Visnyk Dnipropetrovs Kogo Derzhavnogo Universytety Vnutrishnikh Sprav. Vol 1. PP 114–117. https://doi.org/10.31733/2078-3566-2023-5-114-117.

القضائي والتحكيم لكنها تفتقر للتنظيم الخاص بالنزاعات السحابية أو الإلكترونية. أما في الاتحاد الأوروبي، فإن التوجيهات الأوروبية مثل التوجيه رقم ٢٠٠٨/ ٥٢/ EC (الوساطة) والتوجيه ٢٠١٣/ ١١/ EU (التحكيم والتسوية البديلة) تؤكد بشكل صريح على دعم آليات التسوية البديلة في النزاعات الرقمية، بما يوفر إطارًا قانونيًّا أكثر وضوحًا ومرونة[١].

وفي مصر، يُعترف بالتحكيم الإلكتروني بوصفه وسيلة مشروعة لفض النزاعات، خاصة في ظل التطور التكنولوجي المتسارع. وقد قضت محكمة النقض المصرية بجواز استخدام وسائل الاتصال الإلكترونية في إجراءات التحكيم، مثل البريد الإلكتروني، طالما تم احترام الضمانات الأساسية لمبدأ المواجهة وحقوق الدفاع[٢].

ومع ذلك، تواجه تنفيذ أحكام التحكيم الأجنبي تحديات، خاصة عندما يتعلق الأمر بعقود نقل التكنولوجيا. فقد رفضت المحاكم المصرية تنفيذ حكم تحكيم أجنبي استبعد تطبيق القانون المصري، معتبرة ذلك مخالفًا للنظام العام، استنادًا إلى المادة ٨٧ من قانون التجارة المصري التي توجب تطبيق القانون المصري في عقود نقل التكنولوجيا.

وفي الكويت، لا يزال التحكيم الإلكتروني يواجه تحديات تشريعية، على الرغم من الاعتراف به وسيلة لفض النزاعات. وقد تناولت دراسة تحليلية نقدية تنفيذ حكم التحكيم الإلكتروني وفقًا لقانون المرافعات الكويتي، مشيرة إلى الحاجة لتطوير الأطر القانونية لضمان فعالية هذه الوسيلة[٣].

كما أثيرت مسألة العقود الإلكترونية في قضية مواطن كويتي ضد تطبيق "سناب شات"، إذ فوجئ بوجود شرط تحكيم في شروط الاستخدام. وقد ناقشت المحاكم الكـــويتية مدى صحة هذه الشروط،

---

(١) يوسف حامد الياقوت & شيخة طراد الطراد. (٢٠٢٥). تنفيذ حكم التحكيم الإلكتروني وفقًا لقانون المرافعات الكويتي بين الواقع والمأمول: دراسة تحليلية نقدية مقارنة. مجلة العلوم القانونية والاقتصادية. مجلد ٦٧. عدد ١. الصفحات ٣١٥-٤٢٥. doi: 10.21608/jelc.2025.410573.

(٢) أحمد شرف الدين (٢٠٢١). ضوابط حجية المحررات الإلكترونية في الإثبات تعليق على تحديثات اللائحة التنفيذية لقانون التوقيع الإلكتروني في ضوء أحكام محكمة النقض. المجلة الدولية للفقه والقضاء والتشريع. مجلد ٢. عدد ١. الصفحات ٩٤ – ١٠٣.

(٣) شرف خالد إبراهيم. (٢٠٢٢). اتفاق التحكيم الدولي المبرم من خلال التطبيقات الإلكترونية: التعليق على قضية "سناب شات" أمام المحاكم الكويتية. مرجع سابق. الصفحات ١١٥ – ١٦٥.

خاصة في ظل اعتبارها عقود إذعان، مما يثير تساؤلات حول رضا المستخدم الحقيقي[١].

وفي الاتحاد الأوروبي، تُولي المحاكم أهمية كبيرة لحماية البيانات الشخصية في سياق النزاعات السحابية. ففي قضية "Allianz SpA ضد West Tankers"، قضت محكمة العدل الأوروبية بعدم جواز إصدار أوامر قضائية تمنع الأطراف من اللجوء إلى محاكم دول أعضاء أخرى، حتى في وجود اتفاق تحكيم، حفاظًا على مبدأ الثقة المتبادلة بين الدول الأعضاء[٢].

كما تناولت المحكمة مسألة النسخ الخاصة في التخزين السحابي، مشيرة إلى أن مزودي خدمات السحابة قد يكونون ملزمين بدفع تعويضات عادلة لأصحاب الحقوق، حسب النظام القانوني لكل دولة عضو في حين أن الحكم يدعم سلامة اتفاقيات التحكيم، إلا أنه يثير مخاوف بشأن فعالية المحاكم الوطنية في إنفاذ مثل هذه الاتفاقيات، مما قد يؤدي إلى نزاعات قضائية داخل الاتحاد الأوروبي. يشير هذا التوتر المستمر إلى الحاجة إلى مبادئ توجيهية أوضح بشأن التفاعل بين التحكيم وأنظمة المحاكم الوطنية[٣].

وعلى الرغم من فعالية الوسائل البديلة، فإن التحديات القانونية تبقى قائمة، أبرزها: مسألة "الاختصاص القضائي" التي تصبح معقدة جدًا في سياق عقود سحابية دولية، وتحديد "القانون الواجب التطبيق" خاصة عند عدم الاتفاق المسبق في العقد. تُضاف إلى ذلك التحديات المتعلقة بالسرية وحماية البيانات، التي تُعد ضرورية في بيئة السحابة حيث تتقاطع المصالح التقنية والتجارية. في ظل هذه التحديات، تتجه التوصيات القانونية إلى تشجيع الأطراف على تضمين عقود السحابة بنودًا واضحة تتعلق بتدرج وسائل حل النزاعات، بدءًا من المفاوضة والتسوية الودية، وصولًا إلى التحكيم أو اللجوء إلى القضاء عند الضرورة، مع تحديد الاختصاص والقانون الواجب التطبيق مسبقًا.

ويتضح من استعراض هذه البدائل القانونية أن النزاعات الناشئة في بيئة التخزين السحابي تتطلب مقاربة قانونية هجينة تتجاوز الوسائل التقليدية وحدها. فاللجوء إلى الوساطة الإلكترونية والتحكيم

---

(١) المرجع السابق. الصفحات ١١٥ – ١٦٥.

(2) Pribetic A. I. (2009). Case Note: Opinion Of Advocate General Kokott in Allianz SpA (formerly Riunione Adriatica Di Sicurta SpA) and Others v West Tankers Inc. (Case C-185/07 delivered on 4 September 2008). Transnational Dispute Management. Vol 6. Is 1. Available through the following link: https://www.transnational-dispute-management.com/article.asp?key=1396. It was viewed on: 1/6/2025

(3) Ibid.

الإلكتروني ولجان الخبرة التقنية يُشكل ضمانة لاستمرارية الأعمال والسرعة في إنهاء النزاعات، وهو ما لا تُوفره دائمًا المحاكم التقليدية. على المستوى العربي، يُوصى بإصدار تشريعات خاصة تُنظم هذه الوسائل، مستلهمة من التجربة الأوروبية، بما يكفل الحماية القانونية للمستخدمين ويحُقق التوازن بين متطلبات الأمان الرقمي والمصالح التجارية.

وعلى الرغم من الترويج الواسع لاستخدام أساليب بديلة مثل التحكيم الإلكتروني أو التفاوض الإلكتروني في النزاعات السحابية، فإن هذه الوسائل قد لا تكون متاحة أو فعّالة في حالات معينة. ويرجع ذلك إلى أن عقود الإذعان غالبًا ما تُقيّد الخيارات البديلة وتفرض قيدًا على اللجوء إلى أي طريقة خلاف القضاء التقليدي، الذي يُعد الإطار الأكثر رسوخًا وحماية للحقوق، لا سيما عند غياب التوازن في القوة التعاقدية بين المزود والعميل.

في ضوء ما تقدم، يتضح أن غالبية النزاعات القانونية الناشئة عن التخزين السحابي تحُل أمام المحاكم التقليدية، كما سبق بيانه في المطلب السابق من ذات المبحث، وليس من خلال أساليب بديلة، وذلك بسبب سيطرة مزودي الخدمة على صياغة العقود، وامتلاكهم مهارات تقنية وقانونية تفوق قدرات العملاء. هذا الواقع يفرض تحديات جديدة تتطلب مراجعة القواعد القانونية المتعلقة بحماية المستهلكين في البيئة الرقمية، وضمان إتاحة سبل عادلة وفعالة لفض النزاعات، بما يكفل توازن مصالح جميع الأطراف.

الخاتمة:

في ختام هذه الدراسة التي تناولت بالنظر والتحليل الجوانب القانونية للنزاعات الناشئة عن استخدام خدمات التخزين السحابي، يتبيّن أن البيئة الرقمية الحالية قد فرضت واقعًا قانونيًّا جديدًا يتطلب استجابات تشريعية مرنة، خاصة في ظل التعقيد التقني والتوزيع الجغرافي للخدمات السحابية، مما يجعل تحديد القانون الواجب التطبيق والجهة المختصة محل جدل وتباين.

ففي المبحث الأول، جرى استعراض ماهية التخزين السحابي من حيث مفهومه، أنواعه، وخصائصه التي تتسم بالعالمية والتجريد عن البنية التحتية التقليدية. وقد تبين أن هذه الخصائص تطرح إشكاليات قانونية، لا سيما في النظم التي لا تزال تعتمد على المعايير الإقليمية أو الجغرافية لتحديد الاختصاص والقانون الواجب التطبيق.

أما المبحث الثاني، فقد تناول التحديات القانونية المرتبطة بالخدمات السحابية، وركز على طبيعة النزاعات القانونية الجديدة التي تطرأ في بيئة غير ملموسة ومتعددة الأطراف والولايات القضائية. وقد أظهرت المقارنة بين التشريعات أن القانون المصري لا يتضمن حتى الآن إطارًا قانونيًّا خاصًّا بتنظيم خدمات التخزين السحابي، ويعتمد غالبًا على قواعد الالتزامات العامة في القانون المدني، وقانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، إلا أنه لا يجيب بدقة على تحديات الاختصاص العابر للحدود.

بينما ينص القانون الكويتي على مبادئ مشابهة للقانون المدني المصري فيما يتعلق بالعقود والمسؤولية، إلا أن الكويت تفتقر إلى تشريع خاص ومتكامل لحماية البيانات في البيئة الرقمية، مما يضع المستخدم ومزود الخدمة في دائرة الغموض التشريعي، لا سيما فيما يخص نقل البيانات أو مسؤولية الفقد والتسريب الإلكتروني.

أما على المستوى الأوروبي، فقد خطت تشريعات الاتحاد الأوروبي خطوات متقدمة، إذ تعد اللائحة العامة لحماية البيانات (GDPR) نموذجًا رياديًّا في فرض التزامات دقيقة على مزودي الخدمات السحابية، سواء فيما يتعلق بالشفافية، أو نقل البيانات، أو تحديد المسؤولية بين المعالج والمتحكم. كما أظهرت الدول الأوروبية مرونة أكبر في اعتماد التحكيم والوسائل البديلة لفض

النزاعات ذات الطابع الإلكتروني، إلى جانب وضوح أكبر في تكييف القواعد الخاصة بالقانون الواجب التطبيق في النزاعات العابرة للحدود.

وفي المبحث الثالث، ناقشت الدراسة القانون الواجب التطبيق وطرق فض النزاعات، وتبيّن أن التعدد التشريعي في الدول محل الدراسة يؤدي إلى تضارب في القواعد القانونية، خاصة في حال عدم وجود اتفاق صريح بين الأطراف على القانون المختار أو المحكمة المختصة. وقد ظهر أن دول الخليج، ومنها مصر والكويت، بحاجة إلى مزيد من التحديث التشريعي على غرار التجربة الأوروبية التي نجحت في مواءمة قواعد حماية البيانات والاختصاص القضائي مع طبيعة الخدمات الرقمية.

وعليه، خلصت الدراسة إلى ضرورة تبني الدول العربية نهجًا تشريعيًّا موحدًا يُعالج فراغات القوانين الحالية بشأن الحوسبة السحابية، مع تعزيز التنسيق مع المبادرات الدولية الأوروبية، وتطوير وسائل فض المنازعات الإلكترونية بشكل يُراعي خصوصية البيئة التقنية. إن التحول نحو بناء إطار قانوني مرن وعابر للحدود هو الطريق الأمثل لضمان حماية الحقوق الرقمية، واستقرار العلاقات التعاقدية في الاقتصاد الرقمي العالمي.

إن النتيجة المحورية لهذه الدراسة تُؤكد على أن التخزين السحابي يفرض واقعاً قانونياً جديداً يتطلب استجابة تشريعية وتنظيمية عاجلة وفعالة من كافة الأنظمة القانونية. لضمان بيئة رقمية آمنة وموثوقة، لا بد من تطوير أطر قانونية شاملة في التشريعين المصري والكويتي، تستلهم من التجربة الأوروبية (GDPR) في معالجة قضايا الاختصاص وتنازع القوانين بوضوح، وتُحدد المسؤوليات بدقة، وتُعزز من حماية البيانات وحقوق المستخدمين، مع الأخذ في الاعتبار المعايير والممارسات الدولية لضمان الانسجام التشريعي وحماية مصالح جميع الأطراف.

نتائج الدراسة:

توصلت الدراسة إلى جملة من النتائج القانونية المهمة، من أبرزها:

١ـ **تعقيد التكييف القانوني وغياب التعريفات الموحدة**: الدراسة أظهرت أن ماهية التخزين السحابي (مفهومه وأنواعه وخصائصه) لا تزال تفتقر إلى تعريف قانوني موحد وواضح في معظم

التشريعات الوطنية. هذا الغياب يُصعّب عملية التكييف القانوني للعلاقة بين المستخدم ومزود الخدمة (هل هي عقد إيجار، خدمة، أو نوع خاص؟)، مما يُشكل أساسًا لعديد من النزاعات.

٢ـ **غياب إطار قانوني خاص في التشريعات العربية**: تبين أن كلًّا من القانون المصري والكويتي لا يتضمنان تنظيمًا قانونيًّا خاصًّا ومباشرًا لخدمات التخزين السحابي، بل يتم التعامل معها في الغالب ضمن القواعد العامة في القانون المدني وقانون العقود. وهذا يُعد قصورًا تشريعيًّا بالنظر إلى تعقيدات البنية السحابية، خاصة فيما يتعلق بتحديد المسؤولية، حماية البيانات، وفض النزاعات.

٣ـ **التميّز الأوروبي في المعالجة التشريعية**: أظهرت التجربة الأوروبية لا سيما من خلال اللائحة العامة لحماية البيانات (GDPR) وجود تنظيم قانوني أكثر نضجًا وتطورًا لمختلف أبعاد خدمات التخزين السحابي، بما في ذلك تحديد المسؤوليات، اشتراطات نقل البيانات، والحق في التقاضي العابر للحدود. وقد أسهم هذا الإطار في تقليل النزاعات أو على الأقل تسهيل التعامل معها.

٤ـ**تعدد مصادر النزاع في التخزين السحابي**: تبين أن النزاعات في البيئة السحابية قد تنشأ بسبب (أ) فقدان البيانات أو تسريبها، (ب) الإخلال بعقود الخدمة، (ج) التضارب بين القوانين الوطنية عند التعامل مع بيانات عابرة للحدود، أو (د) عدم توافق الأطراف على القانون الواجب التطبيق أو المحكمة المختصة.

٥ـ **أهمية الإرادة التعاقدية في إدارة المخاطر**: توصلت الدراسة إلى أن معظم التحديات القانونية يمكن تقليصها إذا تضمن عقد الخدمة السحابية بنودًا واضحة بشأن؛ القانون الواجب التطبيق، المحكمة المختصة، حدود المسؤولية، حماية البيانات، والإجراءات المتبعة في حال الخلاف. غير أن كثيرًا من العقود السحابية تكون نمطية، مما يُضعف من مركز العميل قانونيًّا.

٦ـ **مكان التحكيم وتأثيره على القانون الواجب التطبيق**: أظهرت الدراسة أن اختيار الأطراف لمكان التحكيم له أثر كبير على القانون الذي سيُطبق على النزاع، خاصة إذا لم يُتفق صراحة على القانون الحاكم. وقد يُفرض تطبيق قانون الدولة التي يقع فيها مركز التحكيم إذا كان يتضمن قواعد آمرة تتعلق بالنظام العام، كما في الحالة الأوروبية.

٧- **ضرورة إعادة صياغة مفاهيم تقليدية**: خلصت الدراسة إلى أن مفاهيم مثل "المكان"، و"المسؤولية"، و"المرفق العام" تحتاج إلى إعادة تفسير في ضوء طبيعة التخزين السحابي، الذي لا يعرف الحدود الجغرافية، ويتطلب نهجًا قانونيًا عابرًا للحدود.

التوصيات:

بناءً على النتائج التي توصلت إليها هذه الدراسة التحليلية المقارنة حول النزاعات القانونية الناشئة عن استخدام خدمات التخزين السحابي، تُقدم التوصيات التالية بهدف تعزيز الإطار القانوني والعملي لبيئة سحابية أكثر أمانًا وفعالية، وتخفيف المخاطر القانونية المحتملة لجميع الأطراف المعنية:

١-على المستوى التشريعي والقانوني (للدول):

- **تحديث وتطوير التشريعات الوطنية**: تُوصي الدراسة بضرورة مراجعة وتحديث القوانين الحالية في كل من مصر والكويت لحماية البيانات الشخصية لضمان شموليتها وفعاليتها في بيئة السحابة. كما يجب أن تتناول التعديلات قضايا مثل تصنيف البيانات (Data Classification)، ومتطلبات سيادة البيانات (Data Sovereignty Requirements)، والضوابط التنظيمية لمقدمي الخدمات السحابية بشكل أكثر تفصيلًا، بما يتجاوز الأحكام العامة.

تفعيل اللوائح التنفيذية إذ يُعد إصدار وتفعيل اللوائح التنفيذية للقوانين الصادرة حديثًا "مثل القانون المصري رقم ١٥١ لسنة ٢٠٢٠" أمرًا حاسمًا لتوضيح آليات التطبيق وتحديد المسؤوليات بدقة، وخصوصًا فيما يتعلق بنقل البيانات عبر الحدود.

كما يُعد وضع معاهدات دولية أو اتفاقيات ثنائية ومتعددة الأطراف أمرًا ضروريًا لمعالجة تحديات الولاية القضائية وتضارب القوانين في الفضاء السحابي. يجب أن تُسهل هذه الاتفاقيات تبادل الأدلة الإلكترونية بين الدول، وتُقدم آليات واضحة للتعامل مع الطلبات الحكومية للوصول إلى البيانات بما يوازن بين متطلبات الأمن القومي وحماية خصوصية الأفراد.

مع النظر في الانضمام أو التكيف مع المبادئ الأساسية للاتفاقيات الدولية المعنية بالجرائم الإلكترونية وحماية البيانات، مثل اتفاقية بودابست بشأن الجرائم الإلكترونية، لتوحيد المعايير.

وذلك لتطوير إرشادات ومعايير أمنية ملزمة (Mandatory Security Standards) خاصة بالخدمات السحابية، تستند إلى أفضل الممارسات الدولية (مثل ISO 27001، NIST Cybersecurity Framework)، وتُطبق على مقدمي الخدمات والعملاء، خاصة في القطاعات الحيوية والحكومية.

توصي الدراسة بإعادة النظر في المفاهيم القانونية التقليدية كـالمكان، الإقليم، والحيازة في ظل المعاملات السحابية التي تتم عبر بنى تحتية موزعة جغرافيًّا وعابرة للحدود.

٢ـ **على مستوى صياغة العقود**: يجب أن تتجاوز العقود البنود العامة وتُفصّل بوضوح الالتزامات الأمنية لمزود الخدمة (Provider's Security Obligations)، بما في ذلك سياسات التشفير، النسخ الاحتياطي، التعافي من الكوارث، وإدارة الهوية والوصول.

وتحديد واضح لـنموذج المسؤولية المشتركة (Shared Responsibility Model): يجب أن تُفصّل العقود مسؤوليات كل من المزود والعميل بشكل لا لبس فيه لتجنب الغموض في حالات خروقات البيانات أو الأعطال. ووضع بنود واضحة لـنقل البيانات عبر الحدود: يجب أن تحُدد العقود الآليات القانونية المعتمدة لنقل البيانات (مثل البنود التعاقدية القياسية إذا كانت تنطبق)، والتزامات المزود بخصوص إخطار العميل بأي طلبات حكومية للوصول إلى بياناته.

وتُوصي الدراسة بتضمين بنود إلزامية للتحكيم أو الوساطة بوصفها خطوة أولى قبل اللجوء إلى التقاضي، مع تحديد الولاية القضائية والقانون الواجب التطبيق ومركز التحكيم بوضوح. ويجب على المؤسسات إجراء تقييمات شاملة لمخاطر الأمن والامتثال قبل التعاقد مع أي مزود خدمة سحابية، بما في ذلك مراجعة شهادات الامتثال (Compliance Certifications) للمزود وسياساته الأمنية. مع مراجعة دورية للعقود والسياسات لضمان مواكبتها للتطورات القانونية والتقنية الجديدة.

٣ـ **على المستوى العملي والتنظيمي**: الاستثمار في تدريب الكوادر الفنية والقانونية داخل المؤسسات على فهم المخاطر القانونية والتقنية للخدمات السحابية، وكيفية إدارة الامتثال لها.

وزيادة الوعي العام والخاص بحقوق حماية البيانات الشخصية والتزامات المؤسسات عند استخدام السحابة.

وتطبيق إجراءات أمنية صارمة داخل المؤسسات، بما في ذلك إدارة التكوينات، والتحكم في الوصول، ومراقبة السجلات (Logging and Monitoring)، واستخدام التشفير لحماية البيانات المخزنة والمعالجة في السحابة. مع وضع خطط فعالة للاستجابة للحوادث الأمنية (Incident Response Plans)، بما في ذلك إجراءات الإبلاغ عن خروقات البيانات للجهات المختصة والأفراد المتضررين وفقًا للقوانين المعمول بها.

وعلى الجهات التنظيمية أن تُقدم إرشادات واضحة للشركات الناشئة والمبتكرين في مجال السحابة، لتمكينهم من تطوير حلول متوافقة قانونيًا منذ البداية ("Privacy by Design").

وينبغي للمشرّعين في كلٍّ من مصر والكويت استحداث تشريع مستقل أو تضمين فصل خاص في قوانين المعاملات الإلكترونية أو حماية البيانات، يُعنى بخدمات الحوسبة السحابية، ويحدّد بوضوح التزامات مقدمي الخدمة، وحقوق العملاء، والمسؤولية القانونية في حال الإخلال بالعقد أو حدوث ضرر.

تُعد هذه التوصيات إطارًا متكاملًا لمعالجة التحديات القانونية المرتبطة بالتخزين السحابي في السياقات المقارنة. من خلال تعزيز التشريعات، تطوير آليات فض النزاعات، والاستثمار في التوعية والبنية التحتية، يمكن لمصر والكويت تحقيق التوازن بين الابتكار التكنولوجي وحماية الحقوق، مع الاستفادة من النماذج الأوروبية لدعم اقتصاد رقمي مستدام. مع حماية حقوق الأفراد والمؤسسات وسيادة الدول في هذا الفضاء المتنامي.

قائمة المراجع: ـ

أولًا: المراجع العربية:-

- أحمد جعفر شاوي. (٢٠٢٠). معايير تحديد القانون الواجب التطبيق على عقود الاستهلاك – دراسة مقارنة. مجلة كلية القانون والعلوم السياسية. العدد السادس. الصفحات ٢٠٩- ٢٠٤١. https://doi.org/10.61279/vrz1pf56.

- أحمد شرف الدين (٢٠٢١). ضوابط حجية المحررات الإلكترونية في الإثبات تعليق على تحديثات اللائحة التنفيذية لقانون التوقيع الإلكتروني في ضوء أحكام محكمة النقض. المجلة الدولية للفقه والقضاء والتشريع. مجلد ٢. عدد ١. الصفحات ٩٤ –١٠٣.

- إيهاب محمد سعيد محمود عويضة العماوي. (٢٠٢٢). القانون الواجب التطبيق على عقود التجارة الدولية. المجلة القانونية. مجلد ١٤. عدد ٦. الصفحات ١٩١٣-١٩٦٦. https://doi.org/10.21608/jlaw.2022.269930.

- سيد أحمد محمود. (٢٠٢٤). حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري رقم ١٥١ لسنة ٢٠٢٠ (حماية البيانات الشخصية المعالجة إلكترونيًا) بين الواقع والمأمول. مجلة العلوم القانونية والاقتصادية. مجلد ٦٦. عدد ١. الصفحات ١٤٣٩-١٤٨٢. doi: 10.21608/jelc.2024.341026

- شرف خالد إبراهيم. (٢٠٢٢). اتفاق التحكيم الدولي المبرم من خلال التطبيقات الإلكترونية: التعليق على قضية "سناب شات" أمام المحاكم الكويتية. جامعة الكويت - مجلس النشر العلمي. مجلد ٤٦. عدد ٤. الصفحات ١١٥ –١٦٥.

- صفاء شكور عباس. (٢٠٢٠). التنظيم القانوني للعقود المركبة في القانون المدني. مجلة الدراسات المستدامة. مجلد ٢. عدد ١. الصفحات ٢١٥-٢٣٠.

- فاطمة الزهراء رباح، بشرى عمور. دور المحكم في تحديد القانون الواجب التطبيق على موضوع النزاع. دفاتر البحوث العلمية. مجلد ١١، عدد ١. الصفحات ٣٥٥-٣٧٣.

https://asjp.cerist.dz/en/article/221872.

- لجنة الأمم المتحدة للقانون التجاري الدولي (الدورة الثالثة والخمسون). (٢٠٢٠). الدليل القانوني إلى الصكوك القانونية الموحدة في مجال العقود التجارية الدولية (مع التركيز على البيع) – مذكرة من الأمانة. ص ٩. ومتاح من خلال الرابط التالي:

https://documents.un.org/doc/undoc/gen/v20/011/76/pdf/v2001176.pdf.

وتم الاطلاع عليه بتاريخ: ٦/ ٧/ ٢٠٢٥.

- مجلس حقوق الإنسان. (٢٠١٨). تقرير المفوّض السامي للأمم المتحدة حول "الحق في الخصوصية في عصر الرقمنة" (A/HRC/39/29). للأمم المتحدة. ومتاح من خلال الرابط التالي: https://docs.un.org/ar/A/HRC/39/29. وتم الاطلاع عليه بتاريخ ٥/ ٧/ ٢٠٢٥.

- محمد عبدالقادر حفني الخطيب. (٢٠٢٤). حرية الأطراف في اختيار القانون الواجب التطبيق على منازعات عقود الوكالة التجارية الدولية. مجلة البحوث القانونية والاقتصادية، تصدر عن كلية الحقوق ـ جامعة المنصورة. مجلد ١٤، عدد ٨٧. الصفحات ١ –٤٨.

https://doi.org/10.21608/mjle.2024.343026.

- محمد محمود على. (٢٠٢٢). تنازع القوانين في مجال إنفاذ اتفاقات التسوية التجارية الدولية طبقاً لمعاهدة سنغافورة للوساطة ٢٠١٨. المجلة الدولية للفقه والقضاء والتشريع. مجلد ٣. عدد ١. الصفحات ١ – ٣١.

- الهيئة العامة للاتصالات وتقنية المعلومات. والمتاح من خلال الرابط التالي: https://citra.gov.kw/sites/ar/Pages/ServiceDetails.aspx?SrvcID=93. وتم الاطلاع عليه بتاريخ ١٥/ ٥/ ٢٠٢٥.

- يوسف حامد الياقوت & شيخة طراد الطراد. (٢٠٢٥). تنفيذ حكم التحكيم الإلكتروني وفقًا لقانون المرافعات الكويتي بين الواقع والمأمول: دراسة تحليلية نقدية مقارنة. مجلة العلوم القانونية والاقتصادية. مجلد ٦٧. عدد ١. الصفحات ٣١٥-٤٢٥. doi: 10.21608/jelc.2025.410573.

ثانيًا: المراجع الأجنبية:

- Sundararajan, G. Liu, M. Starke, R. K. Moorthy & C. Irwin. (2024). Networked Microgrid Ownership, Data, and Control Implications: Challenges and Open Questions. 2024 IEEE Power & Energy Society General Meeting (PESGM). Seattle, WA, USA. PP 1-5. doi: 10.1109/PESGM51994.2024.10688903.
- Adebola Folorunso, Olufunbi Babalola, Chineme Edgar Nwatu & Adebisi Adedoyin. (2024). A comprehensive model for ensuring data compliance in cloud computing environment. World Journal of Advanced Research and Reviews. Vol 24. Is 2. PP 1983–1995. https://doi.org/10.30574/wjarr.2024.24.2.3514.
- Alugoju N. R. (2024). Data Protection in the Cloud: Ensuring Security and Compliance for Organizational Data. International Journal for Research in Applied Science and Engineering Technology. Vol 12. Is 12. PP 1590–1596. https://doi.org/10.22214/ijraset.2024.66087.
- Anil Kumar Reddy Avula. (2024). Understanding Cloud Computing: How Data Storage Works in the Cloud. International Journal For Multidisciplinary Research. Vol. 6. Is 6. https://doi.org/10.36948/ijfmr.2024.v06i06.33472.
- Anithakumari S., Chandrasekaran K. (2017). Negotiation and Monitoring of Service Level Agreements in Cloud Computing Services. In: Satapathy S., Bhateja V., Joshi A. (eds) Proceedings of the International Conference on Data Engineering and Communication Technology. Advances in Intelligent Systems and Computing. Springer, Singapore. Vol 469. https://doi.org/10.1007/978-981-10-1678-3_62.
- Antu A. D., Kumar A., Kelley R. & Xie B. (2022). Comparative Analysis of Cloud Storage Options for Diverse Application Requirements. In Lecture Notes in Computer Science. Springer International Publishing. PP 75–96. https://doi.org/10.1007/978-3-030-96326-2_6.
- Ashwini Kumar. (2023). The Digital Personal Data Protection Bill 2022 in Contrast with the EU General Data Protection Regulation: A Comparative Analysis. International Journal For Multidisciplinary Research. Voll 5. Is 2. https://doi.org/10.36948/ijfmr.2023.v05i02.2534.
- AVSIYEVYCH A. (2024). PROSPECTS OF INFORMATION TECHNOLOGY USE IN INTERNATIONAL COMMERCIAL ARBITRATION DISPUTE RESOLUTION. Naukovyy Visnyk

Dnipropetrovs Kogo Derzhavnogo Universytety Vnutrishnikh Sprav. Vol 1. PP 114–117. https://doi.org/10.31733/2078-3566-2023-5-114-117.

- Bala Akhileswar, A., Kumar Chelluboyina, Y., Vardhan Boya, H., Rao, K. V. & Siva Krishna C. N. (2024). An Analysis of Managing the Cloud: Obstacles and Solutions for Efficient Administration and Protection. International Journal of Innovative Science and Research Technology (IJISRT). Vol 9. Is 8. PP 2537–2544. https://doi.org/10.38124/ijisrt/ijisrt24aug1487.
- Berman P. S. (2018). Legal Jurisdiction and the Deterritorialization of Data. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3134782.
- 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. Is 1. https://doi.org/10.1093/jlb/lsab007.
- Byali R., Jyothi Ms. & Shekadar M. C. (2022). Design and Analysis of Cloud Data's Multi-Layer Security Protection. International Journal of Research Publication and Reviews. Vol 3. Is 8. PP 173–175. https://doi.org/10.55248/gengpi.2022.3.8.5.
- Chakraborty A. (2014). The Conflicting Economic Views Emerging from the Microsoft Antitrust Case: Literature Review. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2373708.
- Chawki M. (2024). An effective cloud computing model enhancing privacy in cloud computing. Information Security Journal: A Global Perspective. Vol 33. Is 6. PP 635–658. https://doi.org/10.1080/19393555.2024.2307637.
- Choi Y. B. (2021). Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases. International Journal of Cyber Research and Education (IJCRE). Vol 3. Is 1. PP 58-64. https://doi.org/10.4018/IJCRE.2021010106.
- Dayanim Behnam & George Edward (2018). Data breach litigation and regulatory enforcement: A survey of our present and how to prepare for the future. In the Cyber Security: A Peer-Reviewed Journal. Vol 1. Is 4. P 301. https://doi.org/10.69554/JJSA8822..
- Dharga Panduranga Kolla. (2024). Automating Real-Time Compliance Data Collection in Cloud Architectures: A Technical Deep Dive.

International Journal For Multidisciplinary Research. Vol 6. Is 6. https://doi.org/10.36948/ijfmr.2024.v06i06.33599.

- Dobrilă M.-C. (2021). Aspecte teoretice şi jurisprudenţiale privind respectarea GDPR la încheierea şi executarea unui contract. ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI (SERIE NOUĂ). ŞTIINŢE JURIDICE. Vol 67. Is 2. PP 93–106. https://doi.org/10.47743/jss-2021-67-4-6.
- Drechsler L. & Kamara I. (2022). "Chapter 13: Essential equivalence as a benchmark for international data transfers after Schrems II". In Research Handbook on EU Data Protection Law. Cheltenham, UK: Edward Elgar Publishing. https://doi.org/10.4337/9781800371682.00022.
- Dritsas E. & Trigka M. (2025). A Survey on the Applications of Cloud Computing in the Industrial Internet of Things. Big Data and Cognitive Computing. Vol 9. Is 2. PP 44. https://doi.org/10.3390/bdcc9020044.
- Eldar O. & Rauterberg G. V. (2022). Is Corporate Law Nonpartisan? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4125863.
- Eswari R., Vamshi A., & Sultan M. S. (2023). An Efficient Data Storage Technique for User Files in Cloud. In 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS). IEEE. PP 1–6. https://doi.org/10.1109/iq-cchess56596.2023.10391609.
- F. Spanca & A. Salihu. (2024). Unveiling the Consequences of Data Breaches: Risks, Impacts, and Mitigation in the Digital Age. 2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE). Kuala Lumpur, Malaysia. PP 1-8. doi: 10.1109/ICECCE63537.2024.10823432.
- G. Megala & S. Prabu. (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. Is 5. PP 1273–1280. https://doi.org/10.17762/turcomat.v12i5.1794.
- Gao H. (2023). Data Sovereignty and Trade Agreements. In Data Sovereignty. Oxford University Press, New York. PP 213–239. https://doi.org/10.1093/oso/9780197582794.003.0010.

- Gavrila S. P. (2024). CHALLENGES AND DIRECTIONS OF THE EUROPEAN REGULATION OF MEDIATION IN CROSS-BORDER DISPUTES. SWS International Scientific Conferences on SOCIAL SCIENCES – ISCSS. Vol 11. PP 115–126. https://doi.org/10.35603/sws.iscss.2024/vs02/04.
- Hammer A., Ohlig M., Geus J. & Freiling F. (2023). A Functional Classification of Forensic Access to Storage and its Legal Implications. Digital Threats: Research and Practice. Vol 4. Is 3. PP 1–14. https://doi.org/10.1145/3609231.
- Helmiawan M. A. & Fadil I. (2020). PRIVATE CLOUD STORAGE IN RURAL'S MANAGEMENT AND INFORMATION SYSTEM USING ROADMAP FOR CLOUD COMPUTING ADOPTION (ROCCA). INTERNAL (Information System Journal). Vol 2. Is 2. PP 172–183. https://doi.org/10.32627/internal.v2i2.85.
- Hongtao Liu. (2024). Optimization and performance improvement of distributed data storage in hybrid storage systems. World Journal of Advanced Engineering Technology and Sciences. Vol 13. Is 1. PP 459–467. https://doi.org/10.30574/wjaets.2024.13.1.0443.
- Hussein B. F., & Mahmoud I. A. (2024). The Legal Implications of a Food Service Provider's Breach of Obligations a Comparative Study. Journal of Ecohumanism. Vol 3. Is 8. PP 9967-9981. https://doi.org/10.62754/joe.v3i8.5609.
- J. B K & T. J. (2022). Data Storage Security and Privacy in Cloud Computing. 2022 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE), Bangalore, India. PP 1-10. doi: 10.1109/ICWITE57052.2022.10176237.
- Jarjis Khalaf Saleh F. & Omar Al Amr S. (2023). Conflict of Legislative and Judicial Jurisdiction in Electronic Contract Disputes - A Comparative Study. Alanya International Congress of Social Sciences. Rimar Academy. PP 101–114. https://doi.org/10.47832/alanyacongress2-10.
- Jennifer Daskal. (2018). Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. Stanford Law Review Online. Vol 71. Available through the following link: https://tinyurl.com/26bue4mo. It was viewed on: 28/5/2025.

- Jiang Y., Li J., Zhang L., Jia Z., Liu W. & Liu C. (2024). Design and Implementation of Secure Cloud Storage System based on Hybrid Cryptographic Algorithm. 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS). IEEE. PP 1–7. https://doi.org/10.1109/iacis61494.2024.10721716.
- Judgment of the Court of 30 November 1976. Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA. Reference for a preliminary ruling: Gerechtshof 's-Gravenhage - Netherlands. Brussels Convention on jurisdiction and the enforcement of Judgment - Article 5 (3) (liability in tort, delict or quasi-delict). Case 21-76. Available through the following link: https://curia.europa.eu/juris/liste.jsf?&num=21/76. It was accessed on 1/10/2025.
- Kaile Sun. (2024). Challenges and Solutions in Cloud Computing Security and Privacy Protection. Journal of Electronics and Information Science. Vol. 9. Is 1. PP 62-68. http://dx.doi.org/10.23977/10.23977/jeis.2024.090110.
- Karagiannis C. & Vergidis K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. Information. Vol 12. Is 5. PP 181(1-16). https://doi.org/10.3390/info12050181.
- Khan A.Q., Matskin M., Prodan R. et al. (2024). Cloud storage cost: a taxonomy and survey. World Wide Web. Vol 27. article number 36. https://doi.org/10.1007/s11280-024-01273-4.
- Khan S., Kabanov I., Hua Y. & Madnick S. (2022). A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. ACM Transactions on Privacy and Security. Vol 26. Iss 1. PP 1–29. https://doi.org/10.1145/3546068.
- Kheira A. (2024). Electronic Arbitration as an Alternative Mechanism for Resolving E-Commerce Disputes. Journal of Lifestyle and SDGs Review. Vol 4. Is 4. P e04292. https://doi.org/10.47172/2965-730X.SDGsReview.v4.n04.pe04292.
- Krishnan S. & Chen L. (2019). Legal Concerns and Challenges in Cloud Computing. (Version 1). arXiv. https://doi.org/10.48550/ARXIV.1905.10868.
- Kun E. (2024). Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks and examining

challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Computer Law & Security Review. Vol 52. P e105931. https://doi.org/10.1016/j.clsr.2023.105931.

- Limam S, Belalem G. (2016). A self-adaptive conflict resolution with flexible consistency guarantee in the cloud computing. Multiagent and Grid Systems. Vol 12. Is 3. PP 217-238. doi:10.3233/MGS-160251
- M. A. Z. Bin Idrus, F. D. A. Rahman, O. O. Khalifa & N. M. Yusoff. (2023). Blockchain-based Security for Cloud Data Storage. 2023 IEEE 9th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), Kuala Lumpur, Malaysia. PP 73-77. Doi: 10.1109/ICSIMA59853.2023.10373457.
- M. Barati & O. Rana. (2022). Tracking GDPR Compliance in Cloud-Based Service Delivery. in IEEE Transactions on Services Computing. Vol 15. Is 3. PP 1498-1511. doi: 10.1109/TSC.2020.2999559.
- M. Harsitha, Lavanya, Manoj Sanikam M. & Mayur Gupta. (2022). A Cloud Storage. International Journal of Advanced Research in Science, Communication and Technology. Vol 2. Is 1. PP 44–52. https://doi.org/10.48175/ijarsct-7064.
- Madhusudhan Dasari sreeramulu. (2024). Analysis of Cloud Computing and Cloud Storage in Mobile Forensics Using the DEMATEL Method. Computer Science, Engineering and Technology. Vol 2. Is 2. PP 33–43. https://doi.org/10.46632/cset/2/2/4.
- Maha A. Sayal. (2023). Private Storage Cloud for Facilitate the Functions of Organizations. International Journal of Information Technology & Computer Engineering. Vol 3. Is 6. PP 43–51. https://doi.org/10.55529/ijitc.36.43.51.
- Marinescu D. C. (2023). Cloud access and cloud interconnection networks. Cloud Computing Elsevier. PP 175–213. https://doi.org/10.1016/b978-0-32-385277-7.00013-0.
- Marinescu D. C. (2023). Cloud data storage. Cloud Computing Elsevier. PP 215–256. https://doi.org/10.1016/b978-0-32-385277-7.00014-2.
- Mathai M. K. & Mathew J. (2024). Cloud storage. In Research Advances in Network Technologies. 1st Edition. PP 137–154. https://doi.org/10.1201/9781003433958-6.

- Mayorova L. A. (2022). Liability clauses in civil law. Siberian Law Herald. Vol 2022. Is 2. PP 75–79. https://doi.org/10.26516/2071-8136.2022.2.75.
- Meglio M. (2020). Embracing Insecurity: Harm Reduction Through a No-Fault Approach to Consumer Data Breach Litigation. Boston College Law Review. Vol 61. Is 3. PP 1223-1269.
- Merkin KC R., Saintier S. & Poole J. (2023). 13. Breach of contract. In Poole's Casebook on Contract Law. Oxford University Press. PP 638–687. https://doi.org/10.1093/he/9780192885081.003.0013.
- Mollakuqe E., Hamdiu E., Fishekqiu N. S., Jakupi S. & Qarkaxhija J. (2024). Comparison of cloud storage in terms of privacy and personal data - Sync, pCloud, IceDrive and Egnyte. Open Research Europe. (version 1; peer review: awaiting peer review). 4. 128. https://doi.org/10.12688/openreseurope.16631.1.
- N. Kushwaha, P. Roguski and B. W. Watson. (2020). Up in the Air: Ensuring Government Data Sovereignty in the Cloud. 2020 12th International Conference on Cyber Conflict (CyCon). Estonia. PP 43-61. doi: 10.23919/CyCon49761.2020.9131718.
- Nanda A. K., Sharma A., Augustine P. J., Cyril B. R., Kiran V., & Sampath B. (2024). Securing Cloud Infrastructure in IaaS and PaaS Environments. In P. Goel, H. Pandey, A. Singhal, & S. Agarwal (Eds.), Improving Security, Privacy, and Trust in Cloud Computing. IGI Global Scientific Publishing. PP 1-33. https://doi.org/10.4018/979-8-3693-1431-9.ch001.
- Nora Ellingsen. (2016). The Microsoft Ireland Case: A Brief Summary. The Lawfare Institute. Available through the following link: https://tinyurl.com/27deccsp. It was viewed on: 13/5/2025.
- Nordic Public Sector Cloud Computing – a discussion paper. (2012). TemaNord. Nordic Council of Ministers. PP 5-56. https://doi.org/10.6027/tn2011-566.
- Odun-Ayo I., Ajayi O., Akanle B. & Ahuja R. (2017). An Overview of Data Storage in Cloud Computing. 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS). IEEE. PP 29–34. https://doi.org/10.1109/icngcis.2017.9.

- Paputungan I. V. (2023). Chapter 17- Explainable renegotiation for SLA in cloud-based system. In Explainable Artificial Intelligence (XAI): Concepts, enabling tools, technologies and applications Institution of Engineering and Technology. PP 329–346. https://doi.org/10.1049/pbpc062e_ch17.
- Pichonnaz P. (2024). Contractual Limitations of Liability and their Impact on Tort Claims. Journal of European Tort Law. Vol 15. Is 1. PP 44-62. https://doi.org/10.1515/jetl-2024-0004.
- Pimenta Rodrigues G. A., Marques Serrano A. L., Lopes Espiñeira Lemos A. N., Canedo E. D., Mendonça F. L. L. d., de Oliveira Albuquerque R., Sandoval Orozco A. L. & García Villalba L. J. (2024). Understanding Data Breach from a Global Perspective: Incident Visualization and Data Protection Law Review. Data. Vol 9. Is 2. PP 27. https://doi.org/10.3390/data9020027.
- Pribetic A. I. (2009). Case Note: Opinion Of Advocate General Kokott in Allianz SpA (formerly Riunione Adriatica Di Sicurta SpA) and Others v West Tankers Inc. (Case C-185/07 delivered on 4 September 2008). Transnational Dispute Management. Vol 6. Is 1. Available through the following link: https://www.transnational-dispute-management.com/article.asp?key=1396. It was viewed on: 13/5/2025
- Qazi F., Kwak D., Khan F. G., Ali F., & Khan S. U. (2024). Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges. Internet of Things. Vol 25. P e101126. https://doi.org/10.1016/j.iot.2024.101126.
- R. S. Sree & K. Raja. (2022). A Review on Forensic Investigation Analysis in Cloud Computing Environments," 2022 1st International Conference on Computational Science and Technology (ICCST). CHENNAI, India. PP 1067-1074. doi: 10.1109/ICCST55948.2022.10040384.
- Rane D., Chourey V., Verma R. & Gupta P. (2022). Consideration of Availability and Reliability in Cloud Computing. In Machine Learning and Optimization Models for Optimization in Cloud. Chapman and Hall/CRC. PP 55–72. https://doi.org/10.1201/9781003185376-4.
- Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast). Available through the following link: https://eur-lex.europa.eu/eli/reg/2012/1215/oj/eng. It was viewed on: 6/7/2025.

- Rognstad O.-A. (2024). Data ownership' ambiguity. In Promoting Sustainable Innovation and the Circular Economy. Routledge. 1st Edition. PP 114–133. https://doi.org/10.4324/9781003309093-7.
- Saini J. S., Saini D. K., Gupta P., Lamba C. S. & Rao G. M. (2022). Cloud Computing: Legal Issues and Provision. Security and Communication Networks. Vol 2022. PP 1–13. https://doi.org/10.1155/2022/2288961.
- Salunke N. R. (2021). Files Storage & Sharing Platform Using Cloud. International Journal for Research in Applied Science and Engineering Technology. Vol 9. Is 11. PP 1338–1344. https://doi.org/10.22214/ijraset.2021.38994.
- Salunke N. R. (2021). Files Storage & Sharing Platform Using Cloud. International Journal for Research in Applied Science and Engineering Technology. Vol 9. Is 11. PP 1338–1344. https://doi.org/10.22214/ijraset.2021.38994.
- Salunke N. R. (2021). Files Storage & Sharing Platform Using Cloud. International Journal for Research in Applied Science and Engineering Technology. Vol 9. Is 11. PP 1338–1344. https://doi.org/10.22214/ijraset.2021.38994.b.
- Seay C., Washington M. & Watson R. J. (2016). Personal Applications of Clouds. In Encyclopedia of Cloud Computing (Wiley). PP 517–523. https://doi.org/10.1002/9781118821930.ch42.
- Seth D., Najana M. & Ranjan P. (2024). Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.68b5dea5.
- Tabatadze T. (2023). The relation of the principle of good faith to the limiting and excluding circumstances of contractual liability. Journal of Contemporary Law. Vol 2. Is 2. PP 170–179. https://doi.org/10.31578/jcl.v2i2.30.
- Tantowi L. & Wijayanti L. (2023). PELUANG DAN TANTANGAN PENYIMPANAN CLOUD STORAGE PADA DOKUMEN DIGITAL. Shaut Al-Maktabah: Jurnal Perpustakaan, Arsip Dan Dokumentasi. Vol 15. Is 1. PP 118–131. https://doi.org/10.37108/shaut.v15i1.803.
- Thi Bao Thu Le, Nicolas Anciaux, Sébastien Gilloton, Saliha Lallali, Philippe Pucheral & et al. (2016). Distributed Secure Search in the Personal

Cloud. EDBT - 19th International Conference on Extending Database Technology, Mar 2016. Bordeaux. France. PP 652-655. hal-01293409

- Tippavajjula A., Pappachan P., Squicciarini A. & Such J. (2024). ACCORD: Constraint-driven Mediation of Multi-user Conflicts in Cloud Services. In Companion Proceedings of the ACM Web Conference 2024 (pp. 1039–1042). WWW '24: The ACM Web Conference 2024. ACM. https://doi.org/10.1145/3589335.3651244.
- Vaibhav Kharose, Himanshu Mevada, Yash Ambarle, Tushar Devre & Shatabdi Bhalerao. (2024). A Cloud-based Multimedia Storage Protection System. International Journal For Multidisciplinary Research. Vol 6. Is 2. https://doi.org/10.36948/ijfmr.2024.v06i02.19320.
- Vankayalapati R. K. (2025). Public clouds: The pillar of scalability and innovation. The Synergy Between Public and Private Clouds in Hybrid Infrastructure Models: Real-World Case Studies and Best Practices. Deep Science Publishing. PP 32-49. https://doi.org/10.70593/978-81-984306-5-6_3.
- Varun Garg. (2024). Overcoming Data Loss Challenges: Best Practices for Backfill and Reprocessing in Distributed Data Systems. International Journal For Multidisciplinary Research. Vol 6. Is 5. https://doi.org/10.36948/ijfmr.2024.v06i05.21547.
- X. Zuo & H. Ding. (2020). Research on Digital Copyright Infringement Based on Cloud Computing Environment. 2020 International Conference on Computer Engineering and Application (ICCEA). Guangzhou, China. PP 128-133, doi: 10.1109/ICCEA50009.2020.00034.
- Y. Zheng, X. Lu, J. Zhai and Y. Zhu. (2023). Reflections on Digital Legislative Management of Privacy under the background of Cloud Service. 2023 International Conference on Intelligent Management and Software Engineering (IMSE). Rome, Italy. PP 100-103, doi: 10.1109/IMSE61332.2023.00027.
- Zhang Y. (2023). Legal Approach to International Cooperation on Cloud Storage of Personal Information. Technium Social Sciences Journal. Vol 40. Is 1. PP 156–165. https://doi.org/10.47577/tssj.v40i1.8341.

- Zuo X. & Ding H. (2020). Research on Digital Copyright Infringement Based on Cloud Computing Environment. Journal of Physics: Conference Series. Vol 1607. Is 1. P e012078. https://doi.org/10.1088/1742-6596/1607/1/012078.
- Валентина Троцька. (2022). ПОЗАСУДОВЕ ВРЕГУЛЮВАННЯ СПОРІВ ЗГІДНО З ЄВРОПЕЙСЬКИМ ЗАКОНОДАВСТВОМ ПРО АВТОРСЬКЕ ПРАВО І СУМІЖНІ ПРАВА В ЄДИНОМУ ЦИФРОВОМУ РИНКУ. Теорія і практика інтелектуальної власності. No 1. PP 35–43. https://doi.org/10.33731/12022.258189.
- 杨健, 王剑 & 杨邓奇. (2014). 版权与数字内容分离的云存储DR M方案. 计算机工程与设计. 年卷 35. 期 7. PP 2330-2334. DOI: 10.3969/j.issn.1000-7024.2014.07.014.
- 王哈琴. (2023). 云存储结构模型及云存储架构的比较研究. 内蒙古民族大学学报 (自然科学). Vol 2013. Is 6. PP 642-645. DOI: 10.3969/j.issn.1671-0185.2013.06.008.

References:

• 'ahmad jaefar shawi. (2020). maeayir tahdid alqanun alwajib altatbiq ealaa euqud alaistihlak - dirasat muqaranati. majalat kuliyat alqanun waleulum alsiyasiati. aleadad alsaadisi. alsafahat 209-2041. https://doi.org/10.61279/vrz1pf56.

• 'ahmad sharaf aldiyn (2021). dawabit hijiat almuharirat al'iiliktruniat fi al'iithbat taeliq ealaa tahdithat allaayihat altanfidhiat liqanun altawqie al'iiliktrunii fi daw' 'ahkam mahkamat alnaqdu. almajalat alduwaliat lilfiqh walqada' waltashriei. mujalad 2. eadad 1. alsafahat 94 - 103.

• 'iihab muhamad saeid mahmud euaydat aleamawi. (2022). alqanun alwajib altatbiq ealaa euqud altijarat aldawliati. almajalat alqanuniata. mujalad 14. eadad 6. alsafahat 1913-1966. https://doi.org/10.21608/jlaw.2022.269930.

• sayid 'ahmad mahmud. (2024). himayat albayanat alshakhsiat alraqamiat wfqan li'ahkam alqanun almisrii raqm 151 lisanat 2020 (himayat albayanat alshakhsiat almuealijat 'ilktrwnyana) bayn alwaqie walmamuli. majalat aleulum alqanuniat waliaiqtisadiati. mujalad 66. eadad 1. alsafahat 1439-1482. doi: 10.21608/jelc.2024.341026

• sharaf khalid 'iibrahim. (2022). aitifaq altahkim alduwalii almubram min khilal altatbiqat al'iiliktruniati: altaeliq ealaa qadia "snab shati" 'amam almahakim alkuaytiati. jamieat alkuayt - majlis alnashr alealmi. mujalad 46. eadad 4. alsafahat 115 - 165.

• safa' shakur eabaas. (2020). altanzim alqanuniu lileuqud almurakabat fi alqanun almadanii. majalat aldirasat almustadamati. mujalad 2. eadad 1. alsafahat 215-230.

• fatimat alzahra' rabah, bushraa eamur. dawr almahkam fi tahdid alqanun alwajib altatbiq ealaa mawdue alnizaei. dafatir albuhuth aleilmiati. mujalad 11, eadad 1. alsafahat 355-373. https://asjp.cerist.dz/en/article/221872.

• lajnat al'umam almutahidat lilqanun altijarii alduwalii (aldawrat althaalithat walkhamsuna). (2020). aldalil alqanuniu 'iilaa alsukuk alqanuniat almuahadat fi majal aleuqud altijariat alduwalia (mae

altarkiz ealaa albayea) - mudhakiratan min al'amanati. s 9. wamutah min khilal alraabit altaali:

https://documents.un.org/doc/undoc/gen/v20/011/76/pdf/v2001176.pdf. watama aliatilae ealayh bitarikhi: 6/7/2025.

• majlis huquq al'iinsani. (2018). taqrir almfwwd alsaami lil'umam almutahidat hawl "alhaqi fi alkhususiat fi easr alraqmanati" (A/HRC/39/29). lil'umam almutahidati. wamutah min khilal alraabit altaali: https://docs.un.org/ar/A/HRC/39/29. watama alatilae ealayh bitarikh 5/7/2025.

• muhamad abdalqadir hafni alkhatib. (2024). huriyat al'atraf fi aikhtiar alqanun alwajib altatbiq ealaa munazaeat euqud alwikalat altijariat alduwaliati. majalat albuhuth alqanuniat walaiqtisadiati, tasdur ean kliat alhuquq jamieat almansura. mujalad 14, eadad 87. alsafahat 1-48. https://doi.org/10.21608/mjle.2024.343026.

• muhamad mahmud ealaa. (2022). tanazue alqawanin fi majal 'iinfadh aitifaqat altaswiat altijariat alduwliat tbqaan limueahadat singhafurat lilwisatat 2018. almajalat alduwaliat lilfiqh walqada' waltashriei. mujalad 3. eadad 1. alsafahat 1 - 31.

• alhayyat aleamat liliatisalat watiqniat almaelumati. walmutah min khilal alraabit altaali:

https://citra.gov.kw/sites/ar/Pages/ServiceDetails.aspx?SrvcID=93. watama aliatilae ealayh bitarikh 15/5/2025.

• yusif hamid alyaqut & shaykhat taraad altaradi. (2025). tanfidh hukm altahkim al'iiliktrunii wfqan liqanun almurafaeat alkuaytii bayn alwaqie walmamuli: dirasat tahliliatan naqdiatan muqaranata. majalat aleulum alqanuniat waliaqtisadiati. mujalad 67. eadad 1. alsafahat 315-425. doi: 10.21608/jelc.2025.410573.

فهـــــرس الموضوعـــــات