

مجلة الحقوق

فصلية علمية محكمة - تصدر عن مجلس النشر العلمي - جامعة الكويت

مدى الحماية القانونية للبيانات الواردة في عقود خدمات الحوسبة السحابية: دراسة في القانون الأردني

الدكتورة/ ليليان رياض إبراهيم العميان



جامعة الكويت
KUWAIT UNIVERSITY

P-ISSN: 1029 - 6069

E-ISSN: 2960 - 2742

العدد ١ - السنة ٥٠

رمضان ١٤٤٧ هـ - مارس ٢٠٢٦ م

مدى الحماية القانونية للبيانات الواردة في عقود خدمات الحوسبة السحابية دراسة في القانون الأردني

الدكتورة/ ليليان رياض إبراهيم العميان*

ملخص

الأهداف: تهدف الدراسة إلى التعرف على مدى قيام المشرع الأردني بحماية البيانات ضمن إطار عقد خدمات الحوسبة السحابية، وذلك من خلال معرفة مفهوم الحوسبة السحابية وأنواعها وأشكال تقديم خدمات السحابة، نظراً لتعقيد الوظيفة التقنية التي تقوم بها تقنيات الحوسبة السحابية متمثلة بتخزين البيانات وحفظها ومعالجتها، وانطلقت الدراسة من مشكلة بحثية تفيد بعدم التطرق لموضوع الحوسبة السحابية كتقنية يتم من خلالها تخزين البيانات وحفظها ومعالجتها فيها، وذلك نظراً لما قد يعتري هذه العقود من مشكلات قانونية ناتجة من عدم وضوح حقوق والتزامات كل من مزود الخدمات السحابية والمستخدم من ناحية البيانات. **المنهج:** استخدمت الدراسة المنهج التحليلي بوصفه المنهج الذي يتناسب مع هدف الدراسة وطبيعتها، وذلك بقراءة نصوص القانون المدني المنظمة للعقود وتطبيقها على خدمات الحوسبة السحابية، وتناول البيانات ومعالجتها وحقوق والتزامات كل من طرفي العقد في الحوسبة السحابية، **النتائج:** وبينت النتائج أنه بينما يضع قانون حماية البيانات الشخصية أحكاماً عامة تتعلق بحماية البيانات، إلا أنه لا يتناول الحوسبة السحابية بشكل صريح كوسيلة لتخزين ومعالجة البيانات. وقد أوصت الدراسة بضرورة تنظيم الحوسبة السحابية ضمن إطار حماية البيانات في التشريع الأردني، وتوضيح توزيع المسؤوليات بين مزودي الخدمة والمستخدمين، ووضع أحكام تعكس الواقع التقني للبيانات السحابية. **الخاتمة:** اختتمت الدراسة ببيان حاجة التشريعات الأردنية لحماية البيانات بشكل كاف ضمن إطار عقود الحوسبة السحابية.

الكلمات المفتاحية: الحوسبة السحابية، البيانات، مزود الخدمة، حماية البيانات الشخصية.

* دكتورة في القانون - كلية الحقوق - الجامعة الأردنية .

الإيميل: Lilian.Alomyan@ncsc.jo/ LilianAlomyan@outlook.com

- تسلم البحث في: ٢٨/١٠/٢٠٢٤، أجاز للنشر في: ١٧/١٢/٢٠٢٤.

حقوق الطبع والنشر محفوظة - مجلس النشر العلمي - جامعة الكويت

للاستشهاد بهذا البحث انظر ص ٣٦٥

المقدمة

الحوسبة السحابية تعتبر إحدى التطورات التكنولوجية البارزة التي غيرت شكل إدارة البيانات والمعلومات والتطبيقات في العالم الرقمي؛ وذلك بقدرتها على تقديم موارد الحوسبة كالتخزين والمعالجة وصنع التطبيقات عبر شبكة الإنترنت، ودون الحاجة إلى امتلاك بنية تحتية مادية محلية، وقد أدت هذه الخدمات إلى وجود مشاكل قانونية تعترى أطراف هذا النوع من العقد، ولا سيما أن له خصوصية معينة تتعلق بحفظ البيانات وتخزينها وحماية حق الخصوصية، وبما يشمل نطاق الخدمات المقدمة في عقود خدمات السحابة كالتخزين، المعالجة وبناء البرامج والمنصات، وبظهور الحوسبة السحابية كنموذج شائع لتقديم خدمات تكنولوجيا المعلومات والاتصالات، وتوفير مجموعة متنوعة من التطبيقات مما يسهم في توفير التكاليف والنفقات المترتبة على حفظ الموارد وتخزينها، أثرت بشكل كبير على حماية البيانات وسريتها ومنع الوصول غير المصرح به إليها، وانتهاك الحق في الخصوصية الذي نادت به معظم التشريعات المحلية كقانون حماية البيانات الشخصية رقم ٢٧ لسنة ٢٠٢٣ والتشريعات الدولية المتمثلة باللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR).

أهداف الدراسة:

تحاول الدراسة تحقيق بعض الأهداف المهمة ومن بينها:

- ١ - التعرف إلى مفهوم الحوسبة السحابية وخصائصها.
- ٢ - التعرف على أنواع نماذج السحابة وأشكال تقديم الخدمات السحابية.
- ٣ - تحديد أركان عقد خدمات الحوسبة السحابية وفقاً للقواعد العامة في التشريع الأردني.
- ٤ - تحديد مفهوم البيانات وأشكالها.
- ٥ - التطرق للحقوق والالتزامات المتعلقة بحماية البيانات ضمن نطاق عقد الحوسبة السحابية في إطار قانون حماية البيانات الشخصية الأردني.

أهمية الدراسة:

- ١ - بيان مفهوم الحوسبة السحابية وخصائصها وأنواعها وأشكالها.
- ٢ - تحديد الأركان الأساسية لعقد خدمات الحوسبة السحابية.

٣ - بيان الحقوق والالتزامات الأساسية في مجال حماية البيانات للأطراف المتعاقدة في عقود الحوسبة السحابية من بداية وجود العقد إلى حين انتهاء عقد خدمات السحابة.

مشكلة الدراسة:

ثمة مبررات أسهمت في وجود مشكلة الدراسة، وخاصة تلك التي تتصل بتحديد الحقوق والالتزامات تجاه مزود الخدمات السحابية والمستخدم في مجال حماية البيانات، ولكن تتمثل الإشكالية الرئيسية في مدى حماية البيانات في الحوسبة السحابية؛ كون قانون حماية البيانات الشخصية لم يتطرق للحوسبة السحابية، وهل من الممكن أن تتناسب عقود الخدمات السحابية مع القواعد العامة أم أنها بحاجة إلى وجود تنظيم تشريعي في قوانين حماية البيانات الشخصية؟ وخاصة أن قانون حماية البيانات الشخصية الأردني رقم ٢٧ لسنة ٢٠٢٣ قد أغفل التطرق لعقود الخدمات السحابية على الرغم من كونها الحاضنة الرئيسية للبيانات.

أسئلة الدراسة:

- ١ - ما هي الأركان الأساسية لعقد خدمات الحوسبة السحابية، ومدى تطابق هذه الأركان مع أركان العقود التقليدية؟
- ٢ - ما هي الحقوق والالتزامات الأساسية في نطاق البيانات وحمايتها للأطراف المتعاقدة في عقود الحوسبة السحابية؟
- ٣ - ما مدى وضوح التزامات مزودي الخدمة فيما يتعلق بحماية البيانات وضمن الخصوصية؟

منهج الدراسة:

سنتناول موضوع الدراسة من خلال المنهج التحليلي، باعتباره المنهج الأكثر تلاؤماً مع طبيعة الدراسة وتحقيق أهدافها، من خلال تحديد وبيان مفهوم الحوسبة السحابية، وبيان خصائصها وأنواعها وأشكالها وتطبيقها على العقود التقليدية، والتطرق لقانون حماية البيانات الشخصية بالنظر إلى محل العقد، وهي البيانات والنظر إلى مدى مواكبة هذه التطورات والابتكارات التقنية، وضمن توافقها مع القوانين السارية وبما يضمن حماية البيانات وحفظ حق الخصوصية.

خطة الدراسة:

- للإحاطة بموضوع الدراسة فقد قُسمت إلى مبحثين رئيسيين، يتفرع كل منهما إلى مطلبين، على النحو الآتي:
- المبحث الأول: ماهية الحوسبة السحابية
 - المطلب الأول: مفهوم الحوسبة السحابية وأنواعها
 - المطلب الثاني: أركان عقد خدمات الحوسبة السحابية
 - المبحث الثاني: حماية البيانات في عقود الحوسبة السحابية
 - المطلب الأول: البيانات في عقود الحوسبة السحابية
 - المطلب الثاني: الالتزام بحماية البيانات في عقود الحوسبة السحابية
 - الخاتمة (النتائج، والتوصيات).
 - قائمة المراجع

المبحث الأول

ماهية الحوسبة السحابية

الحوسبة السحابية تُعنى في الأساس بالاستعانة بمصادر خارجية لعمليات مراكز البيانات أو التطبيقات أو يملكها "مزود موارد الحوسبة السحابية" وهو ما يطلق عليه مقدم الخدمة أو مزود خدمة سحابية، بحيث يوفر هذا المزود نماذج وأنواع خدمات سحابة لاستضافة الموارد والتي تشمل تخزين البيانات أو التطبيقات أو القيام بأعمال وبأنواعها المختلفة، مقابل أن يقوم المستخدم أو متلقي الخدمة بدفع قيمة ما يستأجره أو يودعه من البيانات في الخوادم أو المساحات التخزينية لدى المزود بشكل دوري، وعادةً ما يتطلب قيام مزودي الخدمة السحابية المستثمرين في مجال الحوسبة السحابية بناء وتوفير مراكز بيانات تابعة لهم، وتوفير مرافق البناء للحوسبة السحابية والطاقة الكهربائية والطاقة الاحتياطية وأنظمة التبريد واتصالات الشبكة، بالإضافة إلى رفوف وكابينات الخوادم ومعدات الشبكات وأنظمة التخزين، وفي هذا المبحث نتناول الحديث عن مفهوم الحوسبة السحابية وخصائصها وأنواعها وأشكال تقديم الخدمات فيها.

المطلب الأول

مفهوم الحوسبة السحابية وأنواعها

حاول العديد من الممارسين في المجالين التكنولوجي والأكاديمي تحديد ماهية "الحوسبة السحابية" بالضبط، ومعرفة الخصائص الفريدة التي تقدمها، وقد عرفها الخبراء في مجال تكنولوجيا المعلومات بتعريفات عامة وواسعة كانت تدور حول أنواع ونماذج الحوسبة المقدمة، وبحسب ما يوفره نوع السحابة من مزايا وأساليب للإدارة والتحكم، فقد تم تعريفها بأنها مجموعة من أجهزة الكمبيوتر المترابطة والافتراضية التي تُقدم كواحد أو أكثر من موارد حوسبية موحدة وفقاً لاتفاقيات مستوى الخدمة Service Level Agreement (SLA) التي يتم تحديدها من خلال التفاوض بين مزود خدمات الحوسبة السحابية والمستخدمين للسحابة^(١)، وكما تم تعريف السحابة بأنها مجموعة كبيرة من الموارد الافتراضية التي يمكن استخدامها بسهولة والوصول إليها مثل الأجهزة ومنصات التطوير؛ لتطوير وبناء التطبيقات والخدمات المختلفة، بحيث يمكن إعادة تكوين هذه الموارد تقنياً بالتكيف مع النطاقات المتغيرة للسحابة؛ مما يسمح بالاستخدام الأمثل للموارد، وعادة ما يتم استغلال هذه الموارد من خلال قواعد الدفع عند كل استخدام، بحيث يتم تقديم الضمانات من قبل مزود خدمة السحابة للبنية التحتية عن طريق اتفاقيات مستوى الخدمة^(٢)، وأيضاً تم تعريفها في النحو المماثل لما سبق ذكره بأنها خدمات قائمة على معدات وأجهزة حاسوبية، بحيث تقدم هذه المعدات والأجهزة سعة الحوسبة والشبكة والتخزين، وتتم إدارتها من قبل المستخدم، بحيث يتحمل هذا الأخير تكاليف البنية التحتية من بناء وإدارة كنفقات التشغيل^(٣).

وقد عرف المعهد الوطني للمعايير والتكنولوجيا الأمريكي National Institute of Standards And Technology (NIST) الحوسبة السحابية بأنها؛ نموذج يتيح الوصول إلى مجموعة مشتركة من موارد الحوسبة مثل (الشبكات والخوادم ومساحات

(١) Peter Mell, Timothy Grance "The NIST Definition of Cloud Computing, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg" 2011, website <https://nist.gov>, visit date 25 Sep 2024.

(٢) Nikhila. K, "Cloud computing" 2022 website <https://vardhaman.org/wp-content/uploads/2022/06/Cloud-Computing.pdf> 1 (1), visit date 14 Jul 2024.

(٣) Rajkumar Buyya, James Broberg & Andrzej Goscinski, "Cloud Computing" (John Wiley & Sons, Inc, USA, First Edition 2011) 45.

التخزين والتطبيقات والخدمات) بسهولة وعند الطلب، ويتم توفيرها بسرعة وبأقل جهد من إدارة الموارد^(٤)، وهو معهد تابع لوزارة التجارة الأمريكية، تتمثل مهمته الأساسية في تعزيز الابتكار والقدرة التنافسية الصناعية في علوم القياس والمعايير والتكنولوجيا، وهي هيئة متخصصة في مجال علوم تكنولوجيا المعلومات.

وفي المملكة الأردنية الهاشمية فقد تم إصدار سياسة متعلقة بالحوسبة السحابية، وذلك كتمهيد للاستفادة من خدمات الحوسبة السحابية على المستوى المحلي، وتحديد المتطلبات التي تمكن الجهات والمؤسسات الحكومية في الأردن من استخدام الحوسبة السحابية، صدرت سياسة المنصات السحابية وخدماتها لسنة ٢٠٢٠، وعرفت الحوسبة السحابية بأنها حلول تكنولوجية تتمثل في إمكانية التأجير للبنى التحتية والبرمجيات والمنصات التكنولوجية المختلفة، بحيث يمكن إدارة الموارد التكنولوجية بكفاءة، وتوفير مرونة عالية، وتوفير النفقات مع تحقيق نتائج أفضل بجهد إداري أقل، وإتاحة خدمات إلكترونية للمستفيدين بشكل أسرع، وتطوير المهارات وتوفير بيئة مناسبة للابتكار وتعزيز نمو الاقتصاد الرقمي^(٥).

وفي جميع الأحوال تُعرف الحوسبة السحابية بأنها "خدمة" تُستخدم لحفظ البيانات والمعلومات من التطبيقات والخدمات الأخرى، إذا قام المستخدم بدفع ثمن ما يستخدمه من السحابة أو الدفع عند الاستخدام، وهي تتمثل في عدة حالات؛ أولها تخزين البيانات أو التطبيقات على خوادم بعيدة في مراكز بيانات تتبع مزود الخدمة، ثانيها معالجة البيانات أو التطبيقات من الخوادم، أما الثالثة فهي الوصول إلى البيانات أو التطبيقات عبر شبكة الإنترنت^(٦) حيث تعمل الحوسبة السحابية على تبسيط وتطوير البرامج بأنواعها والتطبيقات والعمليات التجارية والوصول إلى الخدمات عبر الإنترنت؛ كونها تعتمد على تكاليف منخفضة، وبالتالي أصبحت نموذجاً لبيئة الأعمال، وذات مرونة يسمح للشركات والمستخدمين مباشرة ضمن نطاق وبيئة الحوسبة السحابية؛ وذلك ما دفع العديد من المؤسسات والشركات بنقل كافة أعمالهم ومشاريعهم إلى الحوسبة لخفض التكاليف التي كانوا سيستخدمونها لولا وجود خدمات الحوسبة السحابية.

(٤) Mell & Grance (footnote num 1) 34.

(٥) وزارة الاقتصاد الرقمي والريادة الأردنية "سياسة المنصات السحابية وخدماتها" (وزارة الاقتصاد الرقمي والريادة، ٢٠٢٠) www.modee.gov.jo الدخول في ٢٠٢٤ Sep ٢٠٢٤.

(٦) Eric Simmon, "Evaluation of Cloud Computing Services Based on NIST SP 800-145" 2018 website <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf> 4.

وبذلك يمكن أن نعرف الحوسبة السحابية على أنها تقنية تسمح للمستخدمين من الأفراد والمؤسسات والشركات بالوصول إلى البيانات والتطبيقات والخدمات وتخزينها عبر شبكة الإنترنت بدلاً من الاعتماد على الخوادم المحلية أو أجهزة الكمبيوتر الشخصية. يوفر الوصول عند الطلب والاستخدام للبيانات وللبنية التحتية والتطبيقات والعمليات بمختلف أنواعها في بيئة حوسبية قابلة للتطوير وقائمة على وجود شبكة الإنترنت مع توفر متطلبات الحماية والأمان لموارد السحابة، وإدارتها بشكل أكثر كفاءة يتيح إمكانية الوصول إلى البيانات باستخدام الدفع أولاً بأول وعند الطلب.

ولتقنية الحوسبة السحابية عدد من الخصائص تميزها نظراً لطبيعة عملها على النحو الآتي^(٧):

أولاً: خدمة عند الطلب (On-Demand Cloud Computing)

حيث توفر الخدمة تحت الطلب للحوسبة السحابية (On-Demand Cloud Computing) الحصول على الخدمات أو الموارد المختلفة مثل الخوادم، التخزين، قواعد البيانات، الشبكات، والبرامج، بشكل فوري وحسب الحاجة، ودون الحاجة إلى شراء أو إدارة البنية التحتية التقليدية؛ حيث يمكن الدفع عند الاستخدام بحيث يقوم المستخدم بدفع مقابل الحصول على تلك الخدمات والموارد.

ثانياً: الأمان والحماية

توفر الحوسبة السحابية مهمة الحفاظ على البيانات بغض النظر عن طبيعتها سواء أكانت حساسة أم غيرها، وكما تضمن الحفاظ على خصوصية الأفراد والمستخدمين والوصول إليها بكل سهولة ويسر، دون أن يشكل ذلك مصدر قلق في الحفاظ على هذه المعلومات والبيانات الخاصة بالمستخدمين.

ثالثاً: الكفاءة في أداء الخدمات Efficiency Measurement Service

وتقوم هذه الخاصية على التأكد من أن مزودي الخدمات في الحوسبة السحابية قادرون على تقديم الخدمات بكفاءة عالية تدعم القدرة على الحفاظ على نظام إدارة مراكز البيانات وخدمات تكنولوجيا المعلومات، وإتاحة الفرصة للمستخدم كي يتولى إدارة بياناته ومعلوماته واحتفاظ بها داخل السحابة بشكل آمن وفعال^(٨).

Souvik Pal, Le, Pattnai Dac- Nhuong & Kumar Prasant, "Cloud Computing Solutions" (John Wiley & Sons, Inc, USA, First Edition 2022) 30. (٧)

Ibid 25.

(٨)

رابعاً: المرونة في الحصول على البيانات

توفر المرونة الموارد التي يريدها المستخدم عند الطلب في الوقت الفعلي الذي يسعى بموجبه إلى الاطلاع على البيانات الخاصة به، وتشمل المرونة أيضاً القدرة على إضافة وإزالة أو زيادة وتقليل موارد الحوسبة من بيانات وتطبيقات، من خلال حذفها أو الإبقاء عليها، وتظهر خاصية المرونة بشكل عام للمستخدمين بالتوسع في المساحة التخزينية التي يحتاجون إليها، تماشياً بحسب الحاجة وبحسب نطاق العمل^(٩).

وتتعدد طريقة تقديم الخدمات في الحوسبة السحابية، وذلك كله يعتمد على متطلبات وشروط الطرف الآخر المتعاقد مع مزود الخدمة، فهناك نماذج نشر في عقود الحوسبة السحابية تشترطها الأطراف المتعاقدة من حيث مدى توفر الخصوصية والأمان والكفاءة؛ ويشمل ذلك نموذج السحابة العامة، ونموذج السحابة الخاصة، ونموذج السحابة الهجينة وهي التي تجمع بين السحابة العامة والسحابة الخاصة، وكما تتعدد أشكال تقديم الخدمة في الحوسبة السحابية، وهي تختلف بناءً على نوع الموارد المقدمة وكيفية استخدامها.

١ - الحوسبة السحابية العامة (Public Cloud Computing) وهي تعني أن يتم توفير البنية التحتية للسحابة للاستخدام المفتوح من قبل عامة المستخدمين، أي أن الفئة المستفيدة من هذا النوع غير محددة، وبإمكان أي شخص أن يستخدم هذا النوع من الحوسبة السحابية، وهي تكون مملوكة أو مُدارة من قبل شركة تجارية أو مؤسسة تعليمية أو حكومية، والمؤسسة بشكل عام أو الشركة هي التي تختار بأن تستخدم هذا النوع بتحويل وتخزين كافة أعمالها وبياناتها ومعلوماتها وكل ما يتعلق بنطاق عملها داخل هذه السحابة، والتي قد تتبع مزود خدمات سحابية خارج حدود الدولة أو موطن إقامة الشخص المستفيد^(١٠).

٢ - الحوسبة السحابية الخاصة (Privet Cloud Computing) وتسمى أيضاً السحابة الداخلية أو المؤسسية، وهي من النوع المتواجد على أنظمة الأجهزة الموجودة داخل مركز بيانات المؤسسات أو الشركات، وهي في الأساس شبكة إنترانت (Intranet) وهي شبكة مكونة من أجهزة الكمبيوتر ومصممة لمجموعة

(٩) Todd Montgomery & Stephen Olson, "Cloud Complete Study Guide" (John Wiley & Sons, Inc., Indianapolis, Indiana, USA, 2011) 67.

(١٠) وزارة الاقتصاد الرقمي والريادة (رقم الهامش ٥).

معينة من الأشخاص المستخدمين، حيث تتم حماية جميع البيانات والخدمات الموجودة داخل السحابة الخاصة بواسطة أنظمة الحماية التقنية^(١١).

٣ - الحوسبة السحابية الهجينة (Hybrid Cloud Computing) هي عبارة عن مزيج من السحابة العامة والخاصة لجهات مستقلة لكنها مرتبطة ببعضها بعضاً، من خلال تقنيات خاصة تتيح عمليات نقل التطبيقات والأنظمة والبيانات ذات مستويات التصنيف العالية، وتخزينها داخل السحابة الخاصة، وإمكانية استخدام السحابة العامة للبيانات والأنظمة ذات مستويات التصنيف المتوسطة والدنيا، ومن الممكن في هذا النوع من السحابة الاحتفاظ ببيانات المؤسسة الحساسة في مكان العمل أو المقر، وفي الوقت ذاته تستخدم المؤسسة تطبيقاً مخصصاً يتطلب استضافة داخلية، وتجمع البيئة السحابية المختلفة بين ميزات كل من السحب العامة والخاصة باستخدام التكنولوجيا التي تسمح بمشاركة البيانات والتطبيقات بينهما، وتمنح السحابة المختلفة الأعمال والبيانات والمعلومات مرونة أكبر، وقدرة أكبر على حفظها ومعالجتها وتخزينها^(١٢).

وتتنوع أشكال خدمات الحوسبة السحابية لتشمل البنية التحتية كخدمة (IaaS)، والمنصة كخدمة (PaaS)، والبرمجيات كخدمة (SaaS)، على النحو الآتي:

١ - خدمة البنية التحتية (IaaS) Infrastructure as a Service وهو بيئة بنية تحتية افتراضية لخدمات الحوسبة السحابية، وبذلك فهي تقنية تحل محل العناصر المادية ذات الصلة بالخوادم والمكان المادي وجدران الحماية والتكاليف المادية الأخرى، ويقدم هذا النوع من الشبكة الافتراضية للمستخدم؛ قوة التخزين، وقابلية السحابة للتطوير، والاستغناء عن مراكز حفظ البيانات، وتكاليف الدعم المادي التي تشمل الصيانة والطاقة والخبرة والموارد البشرية اللازمة لعملية التشغيل^(١٣).

٢ - خدمة النظام الأساسي (PaaS) Platform as a Service وهي أوسع وأكثر تعقيداً؛ كونها توفر عمليات التطوير والاختبار والصيانة، وتتبع الإصدارات

(١١) Vincent Fogarty & Sophia Flucker, "Data Centre Essential" (John Wiley & Sons Ltd, USA, First Edition 2023)145.

(١٢) Pal & others (footnote num 7) 25.

(١٣) James P Martin & Harry Cendrowski, "Cloud Computing and Electronic Discovery" (by John Wiley & Sons, Inc, Hoboken, USA, Edition one 2014) 56.

والتغييرات وأداء إجراءات وعمليات أخرى تتعلق بإنشاء البرامج، وتوفر (PaaS) بشكل عام وضع حماية يتم تكوينه لاختبار البرامج وميزات إدارة المشاريع وبيئة نشر تمكن المستخدمين من طرح أعمالهم وتطبيقاتهم المستندة إلى السحابة، ومن الأمثلة على سحابات (PaaS) سحابة Amazon Web Services (AWS) وMicrosoft Azure.

خدمة البرمجيات Software as a Service (SaaS) وتسمى أحياناً البرامج عند الطلب أو المستضافة، يستضيف مزود خدمة البرامج التطبيقات في مركز البيانات الخاص به، وفي معظم الحالات يصل المستخدم إليها عبر مستعرض ويب أو واجهة مستخدم مخصصة يتم تنزيلها على كمبيوتر المستخدم، حينها يتم تشغيل البرامج والتطبيقات على أجهزة الكمبيوتر المضيفة والتي يتم الوصول إليها عبر شبكة الإنترنت، وتستهدف خدمة (SaaS) بشكل عام قطاعات الأعمال وشركات القطاع الخاص، وتوفر برامجها وتطبيقاتها بموجب اشتراك يُدفع لفترات دورية وبحسب الاستخدام مثل Salesforce أو SAS أو الدفع عند كل استخدام^(١٤).

ولكون خدمات الحوسبة السحابية فريدة من نوعها نظراً لطبيعتها غير المادية والبنية التحتية التكنولوجية؛ فإن ذلك يتطلب البحث في أركان عقود خدمات السحابة الأساسية في المطلب الثاني.

المطلب الثاني

أركان عقد خدمات الحوسبة السحابية

تتضمن عقود خدمات الحوسبة السحابية خدمات افتراضية، وهي وسيلة مبتكرة للوصول إلى الموارد التقنية دون الحاجة إلى امتلاك أو إدارة الأجهزة والتطبيقات أو البرامج المتخصصة، وكما يلتزم مزودو الخدمة السحابية بحماية البيانات وضمان السرية والخصوصية وفقاً للعقود المبرمة مع المستخدمين، وبذلك نستعرض أركان عقد خدمات الحوسبة السحابية وفقاً للقواعد العامة الواردة في القانون المدني الأردني^(١٥).

Pal & others (footnote num 7) 25.

(١٤)

(١٥) القانون رقم ٤٣ لسنة ١٩٧٦ القانون المدني الأردني.

الفرع الأول الرضا

إن إبرام العقود السحابية في الأساس يتم نتيجة التقاء إرادة الأطراف، بناء على إيجاب وقبول، وغالباً ما توجد هذه العقود بين الشركات والمستخدمين المستهلكين في مجال العقود التجارية، بحيث يتم تزويد المستخدم بالشروط والأحكام التعاقدية، ويتم التعبير عن موافقة المستخدم إما من خلال النقر المزدوج؛ نقرة أولى للتحقق من صحة الطلب، ونقرة ثانية لتأكيد الطلب، أو بإرسال رسالة أو عبر البريد الإلكتروني أو غيرها من تلك الوسائل.

وفيما يتعلق بالإيجاب فإن من يقدم الإيجاب عادة هو مقدم الخدمة أو مزود الخدمة، والذي يصدر منه القبول هو المستخدم لخدمات السحابة، وفي الإيجاب عادة ما يقوم مزود الخدمة بتحديد الشروط التي يتم بموجبها توفير الخدمات السحابية، مثل مساحة تخزين البيانات أو البرامج أو البنية التحتية أو المنصات للمستخدم، بحيث يتم تقديم هذا الإيجاب عن طريق اتفاقيات الخدمة المتاحة على المنصات الرقمية لمزودي خدمات الحوسبة السحابية، مثل أمازون (AWS) ومايكروسوفت (Microsoft) حيث يتيح هذان المزودان اتفاقيات شروط الخدمة على موقعهما الإلكتروني^(١٦)، أما القبول فإنه يصدر عندما يقوم المستخدم بالموافقة على الشروط التي يحددها مزود الخدمة، وذلك بالدخول إلى الموقع الإلكتروني لمزود الخدمة وطلبه الحصول على الخدمة، بحيث يتم ذلك عن طريق النقر فوق زر "أوافق" أو "أقبل" على الاتفاقية، ومن ثم استكمال باقي الإجراءات التعاقدية على شبكة الإنترنت^(١٧)، وهذه الحالة تتطابق مع ما ذهب إليه القانون المدني في نص المادة ٩٣ والتي جاء فيها: "التعبير عن الإرادة يكون باللفظ وبالكتابة وبالإشارة المعهودة عرفاً ولو من غير الأخرس، وبالمبادلة الفعلية الدالة على التراضي، وباتخاذ أي مسلك آخر لا تدع ظروف الحال شكاً في دلالة على التراضي"، حيث ينطبق على القبول في هذه العقود باتخاذ أي مسلك آخر لا يدع مجالاً للشك بصور القبول.

وقد أثّرت آراء حول اعتبار عقود خدمات الحوسبة السحابية عقود إذعان، والتي تفرض على المستخدم التسليم بالشروط التي يضعها مزود الخدمة، نظراً لغياب

Amazon, AWS Service Agreement, Website of Amazon <https://aws.amazon.com> visit date 20 Sep 2024. (١٦)

Martin & Cendrowski (footnote num 13) 78. (١٧)

التفاوض بين الطرفين وخصوصاً من المستخدم أو المستفيد من خدمات السحابة^(١٨)؛ وهذا قول غير دقيق حيث من المعلوم أن عقود الإذعان لا تقتصر فقط على التسليم بالشروط التي يضعها مزود الخدمة، وإنما قد يرافقها عدم منح الطرف الآخر من العقد فرصة حقيقية للمفاوضة بشأن شروطه، وعند النظر في عقود خدمات الحوسبة السحابية نرى أنه من الممكن أن ينظر إليها على أنها عقود إذعان، إلا أنها لا تعتبر كذلك؛ كون ذلك قد يتوقف على ما إذا كان الطرف المتعاقد الآخر وهو المستخدم في موقع يخوله قبول العقد أو رفضه بحرية، فالمزود لخدمات السحابة عندما يضع شروطاً عقدية موحدة تعتمد على نوع الخدمة، كما هو الحال للشروط التعاقدية التي تضعها شركة أمازون (AWS) أو Microsoft Azure، فإن ذلك لا يعني توفر الإذعان في مثل هذه العقود، حيث من الممكن أن يرفض المستخدم التعاقد واللجوء إلى مزود خدمات سحابية آخر بالشروط التي يراها متلائمة مع نوع الخدمة التي يرغب في استخدامها والتفاوض على شروط الخدمة، كما أنه في الوقت ذاته تتمتع الحكومات والشركات الكبرى عند التعاقد مع مزودي خدمات السحابة بسيطرة أكبر على مزود الخدمة إلى الحد الذي قد يؤثر على مصالح مزودي الخدمة.

وبذلك يمكن القول إن ركن الرضا في عقود السحابة يعد من أهم أركان العقد لضمان صحته ونفاذه، وبدونه فإنه لا وجود حتماً لعقد الحوسبة السحابية، وذلك يتطلب وجود رضا كامل وصحيح من الطرفين المتعاقدين على شروط العقد ومحتوياته، بما يشمل تفاصيل الخدمة المقدمة والتزامات كل طرف.

الفرع الثاني

المحل

تنص المادة ١٥٧ من القانون المدني على أنه: "يجب أن يكون لكل عقد محل يضاف إليه"، وركن المحل في عقد الحوسبة السحابية يمثل العنصر الأساسي الذي يدور حوله التعاقد، وهي الموارد والخدمات التقنية التي يلتزم مزود الخدمة بتقديمها للطرف الآخر المستفيد، مثل استضافة البيانات وتخزينها وحفظها ومعالجتها إذا توفر هذا الشرط، وأيضاً توفير البنية التحتية الافتراضية، أو إتاحة البرمجيات والتطبيقات عبر شبكة الإنترنت، كما ينبغي أن توفر مجموعة الموارد على أساس الدفع عند الطلب

(١٨) القانون رقم ٤٣ لسنة ١٩٧٦ القانون المدني الأردني، المادة ١٠٤، تنص المادة ١٠٤ بقولها: "القبول في عقود الإذعان يقتصر على مجرد التسليم بشروط مقررّة يضعها الموجب ولا يقبل مناقشة فيها".

والاستخدام، وبذلك تنص المادة ٢/١٥٨ من القانون المدني على أن المحل يصح أن يكون عيناً أو منفعة أو أي حق مالي آخر، كما يصح أن يكون عملاً أو امتناعاً عن عمل، وفي عقود السحابة تتفاوت متطلبات تقديم الخدمة تبعاً لنوع نموذج النشر ونوع الخدمة المقدمة للمستخدمين، وتوفر الحوسبة السحابية مرونة وسرعة عند تقديم الخدمات، وذلك كله يعتمد على معالجة البيانات، حيث يتم تصنيف البيانات في قاعدة البيانات السحابية على أنها بيانات سرية أو غير سرية، وسواء أكانت منظمة أم غير منظمة، كما يتم استخلاص وتحديد البيانات الكبيرة والصغيرة، وذلك كله عند استخدام السحابة، حيث عادة ما تحتاج البيانات إلى تخزينها بشكل أكثر مرونة ليتم استخلاصها وتحليلها ومعالجتها، ومن ثم تحويلها إلى معلومات؛ وهذا يستدعي إيجاد أفضل الطرق لمعالجة هذه البيانات وتحليلها، الأمر الذي سيتطلب استخدام خدمات الحوسبة السحابية بما يتناسب مع نموذج النشر ونوع الخدمة في السحابة.

البيانات هي "الأرقام أو الحروف أو الرموز أو الأشكال أو الأصوات أو الصور أو الرسومات التي ليست لها دلالة بذاتها" (المادة ٢ من كل من قانون الأمن السيبراني لسنة ٢٠١٩^(١٩) وقانون الجرائم الإلكترونية لسنة ٢٠٢٣^(٢٠))، والمعلومات والتي تم تعريفها على أنها "البيانات التي تمت معالجتها وأصبحت لها دلالة"، وغالباً ما ينظر إلى البيانات على أنها المصدر الذي يمكن من خلالها الحصول على المعلومات أو المعرفة العلمية المتحصلة منها، ويتم تخزين البيانات فعلياً وقياسها بوحدة القياس (Byte) البايت، فالبيانات هي مجموعة من الأرقام والصور والحقائق والأحداث والمعاملات الخام التي يتم إنشاؤها وجمعها وتسجيلها وتخزينها من دون معالجتها، وتتكون البيانات كما ورد في التعريف السابق ذكره من أرقام وأحرف (أي أبجدية ورموز خاصة) تستخدم لتسجيل تلك المعاملات والحقائق والأحداث حول الأنشطة التي تحدث في بيئة معينة، والمعلومات هي البيانات المعالجة، حيث يتم الحصول عليها بعد خضوع البيانات لمجموعة من عمليات المعالجة بشكل يجعل من المعلومات المُستخرجة من البيانات معلومات يمكن الاعتماد عليها في مخرجات ذات معنى^(٢١).

(١٩) قانون رقم ١٦ لسنة ٢٠١٩ الأمن السيبراني.

(٢٠) قانون رقم ١٧ لسنة ٢٠٢٣ الجرائم الإلكترونية.

(٢١) Kuan W Hon, Christopher Millard & Ian Walden, "Negotiating Cloud Contracts; Looking at Clouds from Both Sides Now" (2012) 16 Stanford Technology Law Review Journal p 88.

الفرع الثالث

السبب

نصت المادة ١٦٥/ب من القانون المدني على: "السبب ١- السبب هو الغرض المباشر المقصود من العقد. ٢- ويجب أن يكون موجوداً وصحياً ومباحاً غير مخالف للنظام العام أو الآداب"، يُشير هذا النص القانوني إلى أن العقود والخدمات التي يتم تقديمها يجب أن يكون لها أساس قانوني واضح ومشروع بتحديد الغرض المباشر المقصود من إبرام عقود خدمات الحوسبة السحابية.

إن تحديد السبب كغرض مباشر مقصود من العقد يؤكد على ضرورة قيام المشروعية في الأهداف أو الغرض المباشر من إبرام عقود خدمات الحوسبة السحابية، وتكون متوافقة مع حقوق الأفراد والمستخدمين، أو من تكون بياناتهم معالجة أو مخزنة لدى الشركات أو المؤسسات الحكومية وغيرها، ونظراً لأن الحوسبة السحابية تنطوي عادة على إجراء معاملات وعقود عابرة للحدود، ويكون العقد مبنياً على وجود وإدارة بيانات حساسة، فقد ظهرت مخاطر تتعلق بشرعية هذه العقود، لا سيما وأنها تخترق حقوق الخصوصية للأفراد والمؤسسات، وهناك عدد من التطبيقات والحالات التي يفترض بموجبها أن يكون السبب في عقود خدمات الحوسبة السحابية قانونياً مشروعاً، وإذا لم تتوفر شرعية السبب والغرض المقصود من التعاقد فإن العقد يكون باطلاً حينها، وفي توفر هذا الشرط، تنص اتفاقية شركة أمازون لتقديم الخدمات على أنه:

"إذا كان المحتوى الخاص بالمستخدم ينتهك القانون، أو ينتهك أو يؤثر على حقوق أي طرف ثالث، أو ينتهك شرطاً جوهرياً من الاتفاقية، بما في ذلك شروط الخدمة أو سياسة الاستخدام المقبول والمحتوى المحظور، فإنه سيتم الإخطار بإزالة المحتوى المحظور، أو إزالته من قائمة الخدمات، أو تعطيل ومنع الوصول إليه، وإذا لم تتم إزالة أو تعطيل الوصول إلى المحتوى المحظور خلال مدة الإخطار يحق لشركة أمازون إزالة أو تعطيل الوصول إلى المحتوى المحظور أو تعليق الخدمات" (٢٢).

وضمن نطاق الحوسبة السحابية فإن معالجة البيانات هي السبب الرئيسي الذي يمكن من خلاله اللجوء إلى هذا النوع من العقود، فالمعالجة وكما عرفها قانون حماية البيانات الشخصية الأردني (٢٣) في المادة ٢ هي:

Amazon (footnote num 16).

(٢٢)

(٢٣) قانون رقم ٢٤ لسنة ٢٠٢٤ حماية البيانات الشخصية، المادة ٢.

عملية واحدة أو أكثر يتم إجراؤها بأي شكل أو وسيلة بهدف جمع البيانات أو تسجيلها أو نسخها أو حفظها أو تخزينها أو تنظيمها أو تنقيحها أو استغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو ربطها ببيانات أخرى أو إتاحتها أو نقلها أو عرضها أو إخفاء هويتها أو ترميزها أو إتلافها أو تقييدها أو محوها أو تعديلها أو توصيفها أو الإفصاح عنها بأي وسيلة كانت.

كما بينت المادة ٧ من القانون ذاته شروط إجراء عملية المعالجة للبيانات وحددتها:

- ١ - أن يكون الغرض منها مشروعاً ومحدداً وواضحاً.
 - ٢ - أن تكون متفقة مع الأغراض التي تم جمع البيانات من أجلها.
 - ٣ - أن تتم بوسائل قانونية ومشروعة.
 - ٤ - أن تستند إلى بيانات صحيحة ودقيقة ومحدثة.
 - ٥ - ألا تؤدي إلى تحديد الشخص المعني بعد استنفاد الغرض منها.
 - ٦ - ألا تؤدي إلى التسبب بضرر للشخص المعني أو تنال من حقوقه بشكل مباشر أو غير مباشر.
 - ٧ - أن تتم بطريقة تضمن سرية المعلومات وسلامتها وعدم حدوث أي تغيير عليها.
- ونتناول لاحقاً حقوق والتزامات كل من طرفي التعاقد في عقود السحابة ضمن نطاق حماية البيانات ومعالجتها، حيث تبين أن هذا النوع من العقود يتسم بتعقيدات تقنية تؤثر على الحقوق، بما يتيح المجال لظهور تحديات قانونية مرتبطة به، وحماية البيانات تعتبر من أهم القضايا التي يجب مراعاتها في عقود الحوسبة السحابية، حيث تكتسب هذه المسألة أهمية متزايدة في ظل تزايد حجم البيانات المتبادلة والمخزنة على السحابة، وهنا يأتي دور التشريعات النازمة لحماية البيانات الشخصية، ونتناول موضوع حماية البيانات في المبحث الثاني.

المبحث الثاني

حماية البيانات في عقود الحوسبة السحابية

تمثل البيانات في عقود الحوسبة السحابية العنصر الرئيسي الذي يتم تخزينه، معالجته، أو نقله عبر السحابة، حيث يجب أن يتضمن العقد توضيحاً دقيقاً حول البيانات، وأن مزود الخدمة لا يملك حق استخدامها إلا وفقاً للشروط المتفق عليها، كما يجب أن ينص العقد على إجراءات حماية البيانات، مثل التشفير والنسخ الاحتياطي، لضمان أمانها، بالإضافة إلى الحفاظ على سريتها ومنع الوصول غير المصرح به. كما ينبغي تحديد كيفية نقل البيانات، سواء في أثناء تقديم الخدمة أو عند إنهاؤها، مع الالتزام بالامتثال للقوانين المتعلقة بحماية الخصوصية كقوانين حماية البيانات الشخصية.

المطلب الأول

البيانات في عقود الحوسبة السحابية

عرف قانون حماية البيانات الشخصية لسنة ٢٠٢٣ في المادة ٢ منه البيانات الشخصية على أنها: "أي بيانات أو معلومات تتعلق بشخص طبيعي ومن شأنها التعريف به بطريقة مباشرة أو غير مباشرة مهما كان مصدرها أو شكلها، بما في ذلك البيانات المتعلقة بشخصه أو وضعه العائلي أو أماكن تواجده"، وكما عرفت البيانات الشخصية الحساسة بأنها:

أي بيانات أو معلومات تتعلق بشخص طبيعي تدل بصورة مباشرة أو غير مباشرة على أصله أو عرقه، أو تدل على آرائه أو انتماءاته السياسية أو معتقداته الدينية، أو أي بيانات تتعلق بوضعه المالي أو بحالته الصحية أو الجسدية أو العقلية أو الجينية أو بصماته الحيوية (البيومترية) أو بسجل السوابق الجنائية الخاص به، أو أي معلومات أو بيانات يقرر المجلس اعتبارها حساسة إذا كان إفشائها أو سوء استخدامها يلحق ضرراً بالشخص المعني بها.

وأن البيانات بحسب القانون هي "البيانات الشخصية والبيانات الشخصية الحساسة"، وبذلك نرى أن القانون يشير إلى البيانات التي تحتاج إلى حماية وتعكس الحق في الخصوصية، وذلك بالتزامن مع تزايد الاعتماد على التكنولوجيا في مختلف

جوانب الحياة، أصبحت مسألة حماية البيانات أكثر إلحاحاً، حيث يتم جمع ومعالجة بيانات الأفراد بطرق متعددة.

فالبيانات الشخصية كما وردت في التعريف تشمل مجموعة المعلومات التي يمكن من خلالها التعرف على شخص معين، مثل اسمه الكامل، عنوانه، رقم هاتفه، أو بريده الإلكتروني. لكن القانون لا يقتصر على المعلومات التي يمكن التعرف بها على الشخص بشكل مباشر، بل يشمل أيضاً تلك المعلومات التي قد تدل على هوية الشخص بطريقة غير مباشرة، مثل بيانات الموقع الجغرافي أو سجل النشاط الرقمي، ونرى أن هذا الشمول والتوسع في تعريف البيانات الشخصية يعكس مدى تعقيد وتعدد مصادر البيانات في العصر الرقمي، نظراً لتزايد الاستخدامات لتكنولوجيا المعلومات، فحتى المعلومات التي قد تبدو غير مهمة قد تُستخدم بالتقنيات الحديثة لتحليل هويات الأفراد، ومن جهة أخرى في تعريف البيانات الشخصية الحساسة، فإن هذا المفهوم يعكس البيانات والمعلومات التي تُعتبر حساسة بشكل خاص، مثل الأصل العرقي، الآراء السياسية، المعتقدات الدينية، الحالة الصحية، وحتى البيانات المالية، وأن الكشف عن هذه المعلومات أو إساءة استخدامها قد يترتب عليه أضرار جسيمة للأفراد، مثل التمييز أو استغلال معلوماتهم بشكل غير قانوني مما يعرضهم لخطر الانتهاك لحقوقهم^(٢٤).

وبذلك نرى أن قانون حماية البيانات الشخصية عند إيراد مفهوم البيانات الشخصية والبيانات الشخصية الحساسة، كان قد هدف من خلال هذا التصنيف إلى توفير حماية مشددة على البيانات الحساسة مقارنة بالبيانات الشخصية الأخرى؛ إذ إن الأضرار الناجمة عن تسريب أو إساءة استخدام هذه البيانات تكون عادة أكثر خطورة. ولذلك، يتطلب التعامل مع البيانات الشخصية الحساسة شروطاً خاصة، مثل ضرورة الحصول على موافقة صريحة من الشخص المعني قبل معالجتها.

وتعد معالجة البيانات وحمايتها في عقود الحوسبة السحابية بوجود قواعد البيانات أحد الاعتبارات المهمة في بيئات الحوسبة؛ فقاعدة البيانات هي عملية تنظيم جمع البيانات وتسمى عملية إدارة قواعد البيانات Database Management Software (DBMS) وهي العملية المسؤولة عن الحفاظ على سلامة وأمن البيانات

(٢٤) Christopher Millard, "Cloud Computing Law" (Oxford University, United Kingdom, British Library Cataloguing in Publication Data Second Edition 2021) 43.

المخزنة في الحوسبة السحابية، واستعادة المعلومات المُعالجة في حالة فشل النظام^(٢٥)، ومن حيث الأصل توفر الحوسبة السحابية البنية التحتية لتخزين كميات كبيرة من البيانات ومعالجتها والوصول إليها بكفاءة وسرعة باستخدام مختلف الأنظمة والمنصات السحابية مثل AWS و Google Cloud و Azure والتي سبق ذكرها؛ حيث يمكن للمؤسسات تخزين كميات هائلة من البيانات دون الحاجة إلى أجهزة مادية، مع الاستفادة من القدرة على التوسع في تخزين البيانات بشكل طردي مع تزايد أعداد البيانات ونموها، وكما يمكن الوصول إلى البيانات الموجودة في السحابة، كما أنها في كثير من الأحيان توفر عمليات النسخ الاحتياطي Back Up مما يقلل من مخاطر فقدان البيانات وتوفرها.

وللبيانات ثلاثة أشكال على النحو الآتي:

- ١ - **بيانات منظمة:** أي البيانات التي يمكن تخزينها والوصول إليها ومعالجتها بشكل منسق، وهناك العديد من الأدوات والتقنيات التكنولوجية المتطورة التي يتم استخدامها ليتم تنظيم البيانات ومعالجتها بشكل تلقائي، بحيث يزداد حجم البيانات في ظل وجود تقنيات متعددة.
- ٢ - **بيانات غير منظمة:** وهي البيانات التي تكون بشكل أو بنية غير معروفة وتكون عشوائية؛ ولذلك سُميت ببيانات غير منظمة، وتشكل البيانات غير المنظمة تحدياً من حيث عدم معالجتها لاستخلاص المعلومات منها كالملفات النصية البسيطة والصور ومقاطع الفيديو وما إلى ذلك.
- ٣ - **بيانات شبه منظمة:** يمكن أن تحتوي البيانات شبه المنظمة على نوعي البيانات اللذين سبق ذكرهما (البيانات المنظمة والبيانات غير المنظمة) وهي بالعادة تكون منظمة في شكلها لكن لا تتم معالجتها أو استخلاص المعلومات منها، ومن الأمثلة على البيانات شبه المنظمة البيانات الموجودة في ملف Extensible Markup Language (XML) وهذا النوع من البرنامج يقوم بتحديد البيانات وتخزينها بطريقة قابلة للمشاركة، ويدعم عملية تبادل المعلومات بين أنظمة الكمبيوتر مثل مواقع الويب وقواعد البيانات والتطبيقات^(٢٦).

Pal & others (footnote num 7) 45.

(٢٥)

Amazon (footnote num 16).

(٢٦)

ونظراً لوجود أعداد مهولة من البيانات والعمليات التي ترافق وجودها في الحوسبة السحابية؛ ظهرت مصطلحات تسونامي البيانات أو انفجار البيانات والذي أدى إلى ظهور ما يسمى بالبيانات الضخمة (Big Data)؛ وتُعرف البيانات الضخمة بأنها عبارة عن بيانات كبيرة الحجم وعالية السرعة وعالية التنوع والاختلاف، تتطلب تقنيات وأدوات مبتكرة ومتقدمة لتحليلها ومعالجتها، بحيث تتيح تحسين عملية الوصول إلى البيانات واتخاذ القرارات بناء على معلومات معالجة ومؤتمتة، وللبيانات الضخمة مجموعات كبيرة من البيانات (منظمة أو غير منظمة) تتم معالجتها للخروج بمعلومات منها؛ تتميز هذه البيانات بأنها تتجاوز القدرات التقليدية للبرمجيات في معالجتها بسبب حجمها وتعقيدها وسرعة تدفقها؛ ومما تجدر الإشارة إليه أن هناك كمية هائلة من البيانات التي تولدها المؤسسات والشركات والأفراد كل ثانية، والتي تحتاج إلى معالجة وحفظ وتخزين، وتقوم البيانات الضخمة بجمع وتخزين وتنظيم البيانات التي سيتم تحليلها بشكل أكبر من قبل الأفراد محليي البيانات للوصول إلى معلومات نهائية مُعالجة، وتُشير الإحصاءات بأن هناك ١ مليار عملية بحث على Google ويتم إرسال ٢٩٤ مليار بريد إلكتروني يومياً، وفي كل دقيقة يتم نشر ٦٥,٩٧٢ صورة على تطبيق Instagram، ويتم إنشاء ٤٤٨,٨٠٠ تغريدة على منصة (X)، ويتم تحميل ٥٠٠ ساعة من مقاطع فيديو من تطبيق YouTube، وعلى وسائل التواصل الاجتماعي تشير الإحصاءات إلى أن ٥٠٠+ تيرابايت من البيانات الجديدة يتم استيعابها في قواعد بيانات موقع التواصل الاجتماعي مثل تطبيق Facebook يومياً، ويتم إنشاء هذه البيانات بشكل أساسي عن طريق تحميل الصور والفيديو وتبادل الرسائل والتعليقات وما إلى ذلك^(٢٧).

لم يذكر قانون حماية البيانات الشخصية الأردني موضوع الحوسبة السحابية كمكان يتم من خلاله تخزين البيانات وحفظها ومعالجتها، وذلك على الرغم من انتشار استخدامها؛ وإنما كان قد ركّز على وسائل حماية البيانات وكيفية حمايتها؛ كونه يعد أمن خصوصية البيانات والتطبيقات على السحابة من أهم اهتمامات المستخدمين والمؤسسات، وإضافة إلى ذلك أن مكان السحب الخارجية (خارج حدود الدول) تثير مخاوف بشأن فقدان التحكم بالبيانات ومشاركتها خارج نطاق وسلطة المستخدمين من المؤسسات والشركات، وتعرضها لمخاوف أمنية قد يؤثر بشكل كبير على

Pal & others (footnote num 7) 66.

(٢٧)

مستخدمي تلك السحابات^(٢٨)، وإضافة إلى ما سبق فإن طبيعة العقد الذي يحكم مزود خدمات الحوسبة السحابية والمستخدم يؤثر على جانب الثقة التي يفترض تواجدها في هذا العقد، بالإضافة إلى تدني مستوى التحكم في البيانات من قبل المستخدم وزيادتها من جانب مزود الخدمة.

وبذلك يعد الالتزام بحماية البيانات الشخصية والحساسة من المتطلبات الأساسية التي يفرضها قانون حماية البيانات الشخصية، حتى وإن كانت تقنيات السحابة غير منظمة في القانون، حيث يفرض القانون على الجهات التي تتعامل مع هذه البيانات أن تتبع معايير محددة لضمان السرية والخصوصية، على سبيل المثال، يجب أن يتم الحصول على موافقة واضحة من الأفراد قبل جمع بياناتهم أو معالجتها، ويجب أن تكون هذه الموافقة مبنية على فهم كامل لكيفية استخدام البيانات، ونبطاولها في المطلب الثاني.

المطلب الثاني الالتزام بحماية البيانات في عقود الحوسبة السحابية

في قانون حماية البيانات الشخصية وهو القانون المعني بحماية البيانات، وعلى الرغم من أن القانون لم يتطرق لموضوع الحوسبة السحابية كونها تعتبر من أهم الوسائل والأدوات التي يتم من خلالها حفظ وتخزين البيانات ومعالجتها، فقد منح القانون مجموعة من الحقوق للمستخدمين الذين يقومون بتخزين بياناتهم والسماح بمعالجتها لدى المسؤول أو المعالج، والذي يكون في غالب الأحيان مزود الخدمات السحابية، وهذا يعني أن المسؤول والمعالج يكون في الوقت ذاته مزود خدمات سحابية، وتكون البيانات في عهده.

وفي نص المادة ٤/أ من قانون حماية البيانات الشخصية "مع مراعاة المادة (٦) من هذا القانون، لكل شخص طبيعي الحق في حماية بياناته، ولا يجوز معالجتها إلا بعد الحصول على الموافقة المسبقة للشخص المعني أو في الأحوال المصرح بها قانوناً"، حيث نرى أن هذه المادة كانت قد أعطت الحق للشخص الطبيعي في حماية بياناته، ولا يمكن معالجتها أو الاطلاع عليها أو الوصول إليها إلا إذا كان مصرحاً له

(٢٨) Saeid.Abolfazli, Lailani Alcantara & others, "Encyclopedia of Cloud Computing" (John Wiley & Sons, Ltd United Kingdom First Edition 2016) 134.

بذلك، وفقاً للوائح والتشريعات التي تخول له ذلك.

وقد ذكرت المادة ذاتها مجموعة الحقوق التي يتمتع بها الشخص المعني؛ والشخص المعني في هذا المقام هو الشخص الطبيعي الذي تتم معالجة البيانات الخاصة به وبحثها ضمن نطاق عقود السحابة، وهذه الحقوق نصت عليها الفقرة (ب) من المادة ذاتها وهي:

- ١ - العلم والاطلاع والوصول إلى البيانات الموجودة لدى المسؤول والحصول عليها.
- ٢ - سحب الموافقة المسبقة.
- ٣ - التصحيح أو التعديل أو الإضافة أو التحديث للبيانات.
- ٤ - تخصيص المعالجة في نطاق محدد.
- ٥ - المحو أو الإخفاء للبيانات وفقاً لأحكام هذا القانون.
- ٦ - الاعتراض على المعالجة والتشخيص إذا كانا غير ضروريين لتحقيق الأغراض التي جمعت البيانات من أجلهما، أو كانا زائدين على متطلباتها، أو تمييزية أو مجحفة أو مخالفة للقانون.
- ٧ - نقل نسخة من بياناته من المسؤول إلى مسؤول آخر.
- ٨ - العلم والمعرفة بأي خرق أو انتهاك أو إخلال بأمن وسلامة بياناته.

وبذلك نرى من خلال التطرق إلى مجموعة الحقوق التي وردت في المادة ٤/أ من القانون مثل العلم بالبيانات والوصول إليها، التصحيح أو الحذف، وسحب الموافقة أو الاعتراض على المعالجة، ظهور قصور واضح في تناول دور خدمات الحوسبة السحابية في عملية معالجة البيانات وتخزينها؛ حيث لم يتم التطرق لمكان تخزين البيانات، وكيفية ضمان حمايتها أو تحديثها عبر خوادم موجودة ومتعددة الجنسيات، أو لمزود واحد يمتلك العديد من الخوادم في دول عدة، كما أن النص الآنف الذكر يغفل الإجراءات المتعلقة بنقل البيانات أو حذفها نهائياً في ظل أنظمة سحابية قد تحتفظ بنسخ احتياطية لفترات طويلة.

بالإضافة إلى ذلك، هذا يستدعي وضع تشريعات واضحة تنظم خدمات الحوسبة السحابية لتنظم الأمور القانونية التي غفل عنها قانون حماية البيانات الشخصية، ومنها

مكان تخزين ومعالجة البيانات والذي يعتبر من أهم القواعد والأحكام التي كان يجدر به التطرق لها، وتلزم مزودي الخدمة بموجب ذلك بتحديد أماكن التخزين والتنسيق الدولي بموجب الاتفاقيات والتشريعات الدولية لضمان حماية البيانات وحقوق الأفراد وفقاً للقواعد الدولية؛ كون عقد السحابة عقداً عابراً للحدود.^(٢٩)

وبالرجوع إلى مجموعة الحقوق الواردة في قانون حماية البيانات الشخصية، سيتم البحث فيها وتناولها كما لو كان المسؤول أو المعالج المعنيان بمعالجة البيانات الشخصية هما مزودي خدمات الحوسبة السحابية، وذلك على النحو التالي ذكره:

أولاً: العلم والاطلاع والوصول إلى البيانات الخاصة بالمستخدم.

هذا الحق إذا ما تم استخدامه ضمن خدمات الحوسبة السحابية فإنه يمنح الشخص المعني القدرة على الاطلاع على جميع البيانات التي يحتفظ بها المزود في سياق الحوسبة السحابية، حيث يمكن أن تكون البيانات موزعة على عدة خوادم أو عدة دول؛ لذلك يجب على مقدمي خدمات السحابة توفير وصول الأشخاص المعنيين إلى بياناتهم الشخصية المخزنة على السحابة؛ كون هذا الحق يضمن أن يكون للأشخاص القدرة على معرفة كيفية معالجة بياناتهم، ومن لديه حق الوصول إليها، وبذلك كان على المشرع الأردني التطرق لمواضيع مكان تخزين البيانات ومعالجتها؛ حتى يتمكن المستخدم من خلالها من الوصول إلى بياناته والاطلاع عليها لمعرفة أي سحابة تم التخزين عليها.

ثانياً: سحب الموافقة المسبقة

في عقود الحوسبة السحابية غالباً ما تعتمد الشركات على موافقة المستخدمين لجمع ومعالجة بياناتهم، يتيح هذا الحق للأشخاص المعنيين إمكانية سحب موافقتهم

(٢٩) قانون CLOUD Act لسنة ٢٠١٨، فعلى سبيل المثال نص قانون CLOUD Act (اختصاراً لـ Clarifying Lawful Overseas Use of Data Act) وهو قانون خاص بالولايات المتحدة الأمريكية صدر لتنظيم الوصول إلى البيانات الإلكترونية المخزنة في بيئات وضمن نطاق خدمات الحوسبة السحابية، سواء أكانت تلك البيانات مخزنة داخل الولايات المتحدة الأمريكية أو خارجها، ويهدف القانون إلى إنفاذ القانون الأمريكي ومكافحة الجرائم. يتيح القانون للسلطات الأمريكية إصدار أوامر قانونية (مثل مذكرات استدعاء) للحصول على بيانات مستخدمين مخزنة في خوادم تديرها شركات أمريكية، حتى لو كانت تلك البيانات موجودة في خوادم خارج الولايات المتحدة. www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf، الدخول في ٥ كانون أول ٢٠٢٤.

في أي وقت والانسحاب من عقد خدمات الحوسبة، وهذا يترتب عليه أن على مزود الخدمة أن يتوقف عن معالجة البيانات عند سحب الموافقة. هذا الأمر يوفر للأفراد مرونة كبيرة في التحكم ببياناتهم، خاصة إذا تغيرت شروط الاستخدام، أو إذا شعروا بأن بياناتهم قد تكون معرضة للخطر.

ثالثاً: التصحيح أو التعديل أو الإضافة أو التحديث للبيانات

هذا الحق كان الأجدر على المشرع الأردني عند التطرق له أن يتيح للأشخاص إمكانية تعديل أو تحديث بياناتهم؛ للتأكد من أن البيانات المخزنة دقيقة ومحدثة في البيئة السحابية، حيث إن مزودي خدمات السحابة ملزمون بإتاحة واجهات سهلة الاستخدام تسمح للأشخاص بتصحيح بياناتهم عند الحاجة؛ حيث يتيح هذا الحق للأشخاص إمكانية تعديل أو تحديث بياناتهم للتأكد من أن البيانات المخزنة دقيقة ومحدثة.

رابعاً: تخصيص المعالجة في نطاق محدد

يمنح هذا الحق الشخص المعني القدرة على تقييد كيفية معالجة بياناته، وفي عقود الحوسبة السحابية قد تكون هناك حالات يرغب فيها الأشخاص في تقييد استخدام بياناتهم ضمن نطاق معين، مثل عدم مشاركتها مع أطراف ثالثة أو استخدامها لأغراض تجارية، وهذا يكون متوفراً ضمن اتفاقيات شروط الاستخدام، وهذا الحق يضمن عدم تجاوز معالجة البيانات للأغراض التي تم جمعها من أجلها.

خامساً: المحو أو الإخفاء للبيانات وفقاً لأحكام القانون

هذا الحق الذي يُعرف أيضاً لدى بعض الدول "الحق في النسيان"، حيث يتيح للأشخاص مطالبة مزودي خدمات السحابة بمحو أو إخفاء بياناتهم الشخصية في حال لم تعد ضرورية للأغراض التي تم جمعها من أجلها، وتطبيق إجراءات فعالة لحذف البيانات بشكل آمن من جميع الخوادم والنسخ الاحتياطية عند طلب المستخدم^(٣٠).

سادساً: الاعتراض على المعالجة والتشخيص إذا كانا غير ضروريين

أخفق المشرع الأردني في قانون حماية البيانات الشخصية؛ حيث لم يتطرق للحوسبة السحابية، ولم يسمح للأفراد بالاعتراض على معالجة بياناتهم إذا كانت غير ضرورية لتحقيق الأغراض التي جمعت من أجلها، ومن المعلوم أن في عقود الحوسبة

Buyya & others (footnote num 3) 67.

(٣٠)

السحابية يقوم العديد من مزودي الخدمات السحابية بمعالجة بيانات المستخدمين والاطلاع عليها دون اللجوء إلى المستخدمين، والإخلال بسياسات حق الخصوصية، حيث من الوارد أن تقوم بعض الشركات بتحليل أو معالجة البيانات بطرق تتجاوز متطلبات العقد، مثل استخدام البيانات في تحليل متطلبات السوق التجاري، أو توجيه البيانات والمعلومات لغايات الدعاية والإعلان، حيث منح القانون للأشخاص الحق في الاعتراض على هذه الممارسات إذا كانت تتعارض مع حقوقهم أو مصالحهم.

سابعاً: نقل نسخة من بيانات الشخص المعني من مسؤول إلى مسؤول آخر

حددت المادة ١٤ من قانون حماية البيانات الشخصية أنه لا يجوز نقل البيانات وتبادلها بين المزدودين أو المعالجين أو أي طرف آخر إلا بعد أخذ الموافقة من قبل الشخص المعني، ويُعرف هذا الحق أيضاً بـ "قابلية نقل البيانات"، والمزودون في هذا المقام هم مقدمو الخدمات السحابية الذين يقومون بتقديم خدمة تخزين البيانات ونقلها من خادم إلى آخر، كما يتيح للأشخاص نقل بياناتهم من مزود خدمات سحابية إلى آخر دون عوائق أو شروط قانونية أو متطلبات قد تعرض الشخص المعني لحرمانه من الوصول أو الحصول على بياناته من مزود الخدمات السحابية، وقد بين القانون أن النقل يتم بموافقة الأشخاص المالكين لتلك البيانات، وعلى أن يحقق النقل مصالح مشروعة، وألا يتم استخدام عمليات نقل البيانات لأغراض تجارية أو تسويق لمنتجات، وهذا الحق يمنح للأشخاص في الوقت ذاته تسهيل الانتقال بين مزودي الخدمات، ويمنح الأشخاص مرونة أكبر في اختيار من يقوم بتخزين بياناتهم وإدارتها^(٣١)، وهذا الحق يعد من أهم الحقوق التي ينبغي توفرها للشخص الطبيعي عند تعاقد مع مزود خدمات السحابة؛ كونه يترتب عليه أن يخضع لقوانين عدة دول تبعاً لوجود الخوادم الخاصة بمزود الخدمات السحابية في هذه الدول، كما هو الحال في شركة مايكروسوفت وشركة أمازون، وبذلك ترى هذه الدراسة أنه كان على المشرع الأردني أن يحمي حقوق الأشخاص عند نقلها من مكان لآخر إذا ما تم تخزينها على السحابة؛ نظراً لخطورة نقل البيانات من مزود سحابة إلى مزود آخر وفي دولة أخرى يطبق عليها قوانين وتشريعات تلك الدولة.

Ibid 68.

(٣١)

ثامناً: العلم والمعرفة بأي خرق أو انتهاك لأمن البيانات

تعد الانتهاكات الأمنية وحوادث الأمن السيبراني من أخطر التهديدات التي تصاحب عملية حفظ وتخزين البيانات أو معالجتها؛ حيث يضمن هذا الحق أن يتم إعلام الأشخاص في حال حدوث أي خرق أو انتهاك أمني يؤثر على بياناتهم الشخصية؛ حيث يكون مزودو خدمات السحابة ملزمين بإخطار المستخدمين والأشخاص المعنيين في حالة تعرض بياناتهم للسرقة أو الاختراق.

ونظراً لما سبق التطرق له، كان ينبغي أن ينص قانون حماية البيانات الشخصية الأردني على وضع مفهوم الحوسبة السحابية بشكل صريح في القانون؛ لتعزيز حماية حقوق الأفراد وضمان أمن بياناتهم، ولكون القانون جاء قاصراً على حماية البيانات بتحديد مكان تخزينها، ولكونها من أهم الشروط والأساسيات التي ينبغي الاتفاق عليها، حيث يجب أن يشمل القانون إلزام مزودي الخدمات السحابية بالإفصاح عن أماكن تخزين البيانات، وضمان امتثالها للقوانين المحلية والدولية، مع التأكيد على حق الأفراد في الوصول إلى بياناتهم أو حذفها بشكل نهائي في السحابة، وعدم استغلال مزودي الخدمات لتلك البيانات بعد حذفها، بما في ذلك النسخ الاحتياطية. كما يتعين إلزام الشركات السحابية بالإبلاغ عن أي خروقات أمنية خلال فترة زمنية محددة، وضمان سهولة نقل البيانات بين مزودي الخدمة مع الحفاظ على سلامتها.

وبالرجوع إلى حماية البيانات، نص القانون على عدة إجراءات لحماية بيانات الأشخاص، وذلك استناداً إلى أحكام المادة ٢٠ من قانون حماية البيانات الشخصية بقولها:

أ - عند حدوث إخلال بأمن وسلامة البيانات من شأنه إحداث ضرر جسيم بالشخص المعني، يتوجب على المسؤول القيام بما يلي:

١ - إبلاغ الأشخاص المعنيين الذين تكون بياناتهم قد تأثرت خلال (٢٤) ساعة من اكتشاف عملية الإخلال، وتزويدهم بالإجراءات اللازمة لتفادي أي عواقب قد تترتب على هذا الإخلال.

٢ - إبلاغ الوحدة خلال (٧٢) ساعة من اكتشاف عملية الإخلال عن مصدر الإخلال وآليته والأشخاص المعنيين الذين تأثرت بياناتهم بهذا الإخلال، وأي معلومات أخرى متوفرة حولها.

ب - يكون المسؤول المتسبب بحدوث الخطأ الجسيم أو التعدي ملزماً بتعويض الشخص المعني.

وبموجب النص السابق فإن قانون حماية البيانات الشخصية لم يوضح إذا كان الانتهاك من مسؤول أو معالج خارج حدود المملكة، وهذا يعد قصوراً من المشرع الأردني، كما هو الحال لمزود خدمات سحابية خارج المملكة والبيانات مخزنة خارج المملكة، وبذلك كان يجدر على المشرع الأردني الانتباه إلى البيانات المخزنة والمعالجة خارج المملكة إذا ما تم انتهاكها أو اختراقها، خاصة إذا ما كانت البيانات حساسة ومتعلقة بالمواطنين الأردنيين، أو كانت بيانات حكومية خاصة بالأفراد.

كما كان قد افترض أن بمجرد حدوث انتهاكات أو إخلال بالسرية أو حق الخصوصية إذا كان لا يترتب عليه ضرر جسيم، فإن المسؤول غير ملزم بتبليغ الأشخاص المعنيين بحماية البيانات، وبالتالي ينتفي العلم لديهم لمعرفة ما إذا كانت بياناتهم قد تعرضت للانتهاكات أو الاختراقات، وبالعكس ذلك فإنه قد اشترط توفر الضرر الجسيم إذا كان الإخلال بأمن وسلامة البيانات يحدث ضرراً جسيماً بالشخص المعني، وبذلك يفهم من هذا النص أن المسؤول هو المعني بتقدير الضرر الجسيم من عدمه، وبالتالي يترتب عليه قيامه بإبلاغ الأشخاص المعنيين أم عدم إبلاغهم، ونتعقد أن هذا الموضوع ينبغي أن يتم تقديره من قبل الوحدة المعنية بحماية البيانات الشخصية في وزارة الاقتصاد الرقمي والريادة، وذلك حتى يتمكن من الابتعاد قدر الإمكان عن تعسف المسؤول ومن بحوزته البيانات في استعمال الحق وتقديره من عدمه.

وفيما يتعلق بالالتزامات وحماية البيانات فقد بينت المادة ١١ من قانون حماية البيانات الشخصية بأنه على المراقب وهو الشخص الطبيعي المعين للإشراف على قواعد البيانات والمعالجة بأن يتولى مجموعة من الالتزامات، ومنها ما هو متعلق بحماية البيانات والتي وردت في البندين الأول والثاني بقولهما الأول مراقبة إجراءات المسؤول المتعلقة بحماية البيانات، والثاني التأكد من إجراء التقييم والفحص الدوري لأنظمة قواعد البيانات ومعالجة البيانات وأنظمة المحافظة على أمن وسلامة حماية البيانات بشكل دوري، على أن يتم توثيق نتائج التقييم، وإصدار التوصيات اللازمة لحماية البيانات، ومتابعة تنفيذ هذه التوصيات، وحيث إن هذه المادة في نطاق عقود الحوسبة السحابية لا تنص عليها معظم العقود، وعادة ما يتولى مزودو الخدمات اتخاذ إجراءات حماية البيانات وتوثيق النتائج دون أن يتم إشراك المستخدمين في معرفة مستوى

الإجراءات المتخذة لحماية بياناتهم، أو معرفة ما هي الإجراءات التي تم اتخاذها. وفي مقابل ما سبق ذكره ينطوي إبرام عقود خدمات الحوسبة السحابية على التزامات قانونية تجاه مزود الخدمة، خاصة تلك المتعلقة بحماية البيانات؛ وتتمثل هذه الالتزامات على النحو التالي:

أولاً: السرية وحق الخصوصية: وقد كفلته النصوص الدستورية في مختلف الدول كالدستور الأردني^(٣٢) حيث نصت المادة ٧ من الدستور الأردني لسنة ١٩٥٢ وتعديلاته ضمن الحريات والحقوق على أن: "١. الحرية الشخصية مصونة، ٢. كل اعتداء على الحقوق والحريات العامة أو حرمة الحياة الخاصة للأردنيين جريمة يعاقب عليها القانون"، كما أن حق الخصوصية وحماية البيانات نصت عليه معظم التشريعات في مختلف الدول بموجب إصدار قوانين خاصة، كما هو الحال في قانون حماية البيانات الشخصية الأردني لسنة ٢٠٢٣، وقانون حق الخصوصية الأمريكي واللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي، ويخضع مزودو الخدمات السحابية عادة إلى القوانين المتعلقة بالخصوصية في الدول التي يقيمون فيها أو يكون مركزهم الرئيسي فيها، حيث يلتزم الأطراف المتعاقدة في عقود خدمات السحابة بالاتفاق على بند خاص متعلق بحق الخصوصية، كما يمكن أن يمتد هذا البند إلى أطراف ثالثة قد تتمكن من الاطلاع على البيانات والمعلومات الموجودة في السحابة، وهذا كله يعتمد على الاتفاق الذي يكون بين الأطراف بتحديد نطاق حق الخصوصية، ويمكن أيضاً أن يأتي الاتفاق على حق الخصوصية إما بصيغة عقود مستقلة، أو بوجود بند في اتفاقيات مستوى الخدمات، أو في شكل اتفاق مرفق بعقد الخدمات السحابية، وبموجب الحالات الوارد ذكرها فقد تكون صريحة أو ضمنية^(٣٣).

وفيما يتعلق بالسرية فإن مزودي الخدمات يمكنهم الوصول بسهولة إلى البيانات، بل والاطلاع عليها، فالبيانات السرية في عقود خدمات السحابة تنقسم إلى نوعين: الأول البيانات والمعلومات التي يفصح عنها المستخدمون في أثناء إجراء المفاوضات مع مزود الخدمة على العقد؛ كالمعلومات المتعلقة بالغرض المقصود من العقد، وسبب

(٣٢) الدستور رقم ١٠٩٣ لسنة ١٩٥٢ الدستور الأردني.

Pal & others (footnote num 7) 150.

(٣٣)

استخدام الخدمة على السحابة، وثانيها البيانات التي تتم معالجتها باستخدام الخدمة في السحابة، وفي كلتا الحالتين قد تتضمن هذه البيانات بيانات شخصية أو حساسة أو بيانات حكومية تؤثر على وضع الدولة السياسي أو الاقتصادي^(٣٤).

وبناء على ذلك، قد يرغب المستخدمون في توقيع ووضع التزامات متعلقة بالسرية، وعدم الإفشاء عن البيانات والمعلومات، والإفصاح عنها من قبل مزودي الخدمات، وتحميل مزودي الخدمات أقصى درجات مستويات المسؤولية، وذلك كله يعتمد على مدى تقبل مزودي تلك الخدمات لوضع الشروط والأحكام التي تثبت مسؤوليتهم عن خرق البيانات وانتهاك سريتها أو الكشف عنها، وبالتالي التعويض عن الأضرار المترتبة على هذا الخرق، وعادة ما تمتد الاتفاقيات المتعلقة بشرط السرية إلى ما بعد نهاية العقد من ٥ إلى ٧ سنوات، وذلك كله يعتمد على طبيعة البيانات وتصنيفها، وما إذا أراد المستخدم البقاء في الاستفادة من الخدمات السحابية إلى أجل غير مسمى^(٣٥).

ثانياً: الالتزام بحماية البيانات: يلتزم مزود الخدمة بحماية بيانات المستخدمين، وفي حالة حدوث خرق للبيانات، فإن مزود الخدمة يلتزم بإخطار المستخدم في الحال، وذلك اعتماداً على الشروط التعاقدية والتشريعات المعمول بها، كما قد يطلب من المزود تشفير البيانات ومنع الوصول غير المصرح به إلى البيانات، وكما يلتزم المزود بالقيام بإجراءات الاتفاق مع المستخدم على اتباع إجراءات تكفل حماية البيانات واستعادتها في حال تأثر الأنظمة والشبكات والمنصات الخاصة بها والخوادم، كالقيام بعمليات النسخ الاحتياطي للبيانات واستعادتها؛ حيث يتولى مزود الخدمة توفير تقنيات النسخ الاحتياطي للبيانات (Backup Data) في العقود السحابية، بحيث يكون المستخدمون مسؤولين عن النسخ الاحتياطي لبياناتهم الخاصة، وأيضاً توفير عمليات استعادة البيانات، بحيث يكون لدى المستخدمين آليات لاستعادة البيانات في حالة الحذف عن طريق الخطأ أو التلف أو فشل الخدمات السحابية لديهم أو تعذر الوصول إليها، ويقدم المزود هذه الخدمات على وجه التحديد بموجب ذلك العقد^(٣٦).

Buyya & others (footnote num 3) 35.

(٣٤)

Zimmeck, Sebastian, "The Information Privacy Law of Web Applications and Cloud Computing" (2013) 29 Santa Clara Computer & High Technology Law Journal 451.

(٣٥)

Millard (footnote num 24) 78.

(٣٦)

كما يقع على عاتق المزود توفير ميزة القابلية لنقل البيانات؛ حيث يجب على المزود تمكين المستخدمين من استرداد بياناتهم سواء عند الطلب أو عند إنهاء العقد، وهذا يتيح لهم إمكانية اللجوء إلى مزودي خدمة آخرين، أو ترحيل بياناتهم إلى خدمات أخرى، وأيضاً فيما يتعلق بحذف البيانات بعد انتهاء العقد، فيكون مزود الخدمة ملزماً بحذف بيانات المستخدم بشكل آمن من أنظمتها وخوادمه، وحذف النسخ الاحتياطية، بما يتماشى مع سياسات الاحتفاظ بالبيانات وحذفها المنصوص عليها بالعقد (GDPR)، وفي مقابل كل ذلك يلتزم المستخدم بالدفع مقابل الخدمات السحابية، ووفقاً لشروط التسعير المنصوص عليها في العقد والتي يضعها مزود الخدمة، وبما يتناسب مع حجم الخدمة التي يقدمها وسعتها ومدتها، وحيث من الممكن أن تشمل هذه الرسوم؛ رسوم الاشتراك والرسوم القائمة على الاستخدام والزيادات المفروضة على تجاوز حدود نطاق ومساحة الموارد المتفق عليها كزيادة مساحات التخزين^(٣٧).

إن الالتزام بهذه القوانين ليس فقط ضرورة قانونية، بل هو عنصر أساسي لضمان ثقة المستخدمين في خدمات الحوسبة السحابية. ويتطلب هذا من مزودي الخدمة توفير آليات صارمة لحماية البيانات مثل التشفير، والتحكم في الوصول، وضمان ألا يتم استغلال البيانات أو مشاركتها بطرق غير مشروعة. وبهذا يكون لعقود الحوسبة السحابية دور محوري في وضع الأسس القانونية لحماية البيانات؛ مما يعزز من التزام الطرفين بمسؤولياتهما تجاه حماية خصوصية البيانات الشخصية، ويضمن الامتثال للقوانين الدولية والمحلية في هذا المجال.

إن انتهاء عقود الحوسبة السحابية، بما في ذلك انتهاء العقد لانتهاء المدة أو للإخلال بالالتزامات التعاقدية، أو حدوث ظروف خارجة عن إرادة الأطراف، قد يؤثر على حماية البيانات بطريقة أو بأخرى، حيث تنتهي عقود خدمات السحابة بعدة طرق نتناولها وفقاً للقواعد العامة على النحو التالي:

أولاً: انتهاء العقد بانقضاء المدة المحددة

حيث يكون الاتفاق منذ بداية العلاقة التعاقدية على مدة محددة لاستمرار تقديم الخدمة، ومع اقتراب نهاية هذه المدة، يتوجب على الأطراف اتخاذ قرارات إما بتمديد العقد أو إنهائه، كما قد ينتهي العقد باتفاق الأطراف، وفي هذه الحالة، يتفق الطرفان

Montgomery & Olson (footnote num 9) 45.

(٣٧)

على إنهاء العقد قبل انتهاء المدة المحددة، ويتطلب هذا الاتفاق في عقود خدمات السحابة تسوية كافة الحقوق والالتزامات المترتبة على العلاقة التعاقدية بين مزود الخدمة والمستخدم، بما في ذلك تسوية الرسوم المستحقة وضمن استعادة البيانات للمستخدم واستردادها^(٣٨).

ثانياً: انتهاء العقد دون تجديد

في حال عدم رغبة أحد الأطراف في تجديد العقد، يجب إشعار الطرف الآخر ضمن فترة زمنية محددة، وفي حالة عدم توجيه إشعار، فإن العقد ينتهي بانتهاء مدته.

ثالثاً: إنهاء العقد قبل انتهاء مدته

يمكن أن يحدث ذلك بناءً على رغبة أحد الأطراف، أو نتيجة لظروف معينة تستدعي ذلك، حينها يحدث الإنهاء بسبب إخلال الطرف الآخر، وفي حال إخلال أحد الأطراف بالتزاماته التعاقدية، يحق للطرف المتضرر إنهاء العقد، أو منح فترة محددة للطرف المخالف لتصحيح الوضع قبل إنهاء العقد^(٣٩).

رابعاً: انتهاء العقد لأسباب القوة القاهرة

يمكن إنهاء العقود في حال حدوث ظروف قاهرة تمنع استمرار العلاقة التعاقدية، وتشمل هذه الظروف الحوادث الحربية أو الكوارث الطبيعية أو حوادث الأمن السيبراني أو التهديدات والهجمات السيبرانية التي تؤدي إلى تعطيل الخدمة بشكل مستمر وتسريب البيانات وتعطل جميع الخدمات، ففي هذه الحالة، قد يتم إعفاء الأطراف من التزاماتهم التعاقدية إذا ثبت أن تلك الظروف خارجة عن إرادتهم، وأنهم لم يتمكنوا من الوفاء بالتزاماتهم رغم اتخاذهم جميع الإجراءات الممكنة. وسنتناول لاحقاً في دراسات أخرى الإشكاليات القانونية المترتبة على تسريب البيانات وانتهاك حق الخصوصية، وتعرض خدمات السحابة لحوادث الأمن السيبراني (المادة ٢٤٧ من القانون المدني).

وعند انتهاء عقد خدمات الحوسبة السحابية فإن هناك مجموعة من الآثار التي تحدث حينها:

Hon., Millard. & Others (footnote num 21) 67.

(٣٨)

Ibid 68.

(٣٩)

أولاً: استعادة بيانات المستخدم

تعد استعادة البيانات من أهم الآثار المترتبة على انتهاء عقد خدمات السحابة؛ حيث يجب معالجتها عند انتهاء العقد، وتشمل بما في ذلك أن يتولى مزود الخدمة تقديم ضمانات قانونية وإجراءات فنية لاسترجاع البيانات المخزنة على الخوادم السحابية، بحيث يجب أن تحدد هذه البنود المدة الزمنية المتاحة لاستعادة البيانات، والإجراءات الفنية المتبعة لذلك، كما يجب أن تضمن العقود عدم إتلاف أو حذف البيانات إلا بعد التأكد من استرجاعها بالكامل من قبل المستخدم^(٤٠).

ثانياً: حالات فقدان البيانات وحماية الخصوصية

في حال لم يتمكن المستخدم من استعادة بياناته بعد انتهاء العقد، قد يُعتبر مزود الخدمة مسؤولاً عن فقدان البيانات، وتنشأ حينها المسؤولية القانونية تجاه مزود الخدمة، وفي هذه الحالة تبرز أهمية حماية الخصوصية بشكل خاص، حيث يتعين على مزود الخدمة اتخاذ التدابير اللازمة لضمان عدم استغلال البيانات الشخصية التي تم تخزينها أو معالجتها في أثناء مدة العقد، وتجنب حذف مزود الخدمة للبيانات الشخصية بموجب التشريعات الدولية والمحلية الموجودة فيها؛ حيث قد يكون مزود الخدمة ملزماً بحذف البيانات الشخصية التي تم جمعها ومعالجتها فور انتهاء العقد، إلا إذا كان هناك سبب قانوني أو تنظيم يسمح بالاحتفاظ بها لفترة أطول، ويضمن هذا الحذف حماية الخصوصية ومنع استخدام البيانات لأغراض غير قانونية وغير مشروعة، كما أن هناك العديد من التشريعات التي تلزم مزود الخدمة بإبلاغ المستخدمين عن الإجراءات التي تم اتخاذها لحذف البيانات، ويجب عليه تقديم ضمانات قانونية بعدم مشاركة أو استغلال تلك البيانات من قبل أي طرف ثالث بعد انتهاء العقد^(٤١).

الخاتمة

في ختام هذه الدراسة، يتضح أن حماية البيانات الشخصية ضمن نطاق عقود خدمات الحوسبة السحابية تشكل تحدياً متزايداً في ظل الاعتماد المتنامي على التكنولوجيا في مختلف القطاعات، وقد تبين أن قانون حماية البيانات الشخصية الأردني لعام ٢٠٢٣ قد وضع إطاراً قانونياً شاملاً لضمان حقوق الأشخاص في التحكم

Montgomery & Olson (footnote num 9) 67.

(٤٠)

Millard (footnote num 24) 86.

(٤١)

ببياناتهم، مثل حق الوصول، التصحيح، سحب الموافقة، والحق في نقل البيانات بين مزودي الخدمة، إلا أنه لم يتطرق بشكل مباشر لموضوع الحوسبة السحابية كحاضنة أساسية يتم حفظ البيانات لديها وتخزينها ومعالجتها، وإنما تناول الأحكام الخاصة بالمسؤول على أساس أنه مزود خدمات السحابة.

النتائج

- ١ - أسهم قانون حماية البيانات الشخصية الأردني لسنة ٢٠٢٣ في وضع إطار قانوني لحماية البيانات للشخص المعني، والحفاظ على حقه في حماية الخصوصية بشكل عام، لكنه في الوقت ذاته لم يتطرق لأحكام الحوسبة السحابية واستخدامها كتقنية يتم من خلالها حفظ وتخزين ومعالجة البيانات، كما أن حماية البيانات ضمن نطاق خدمات الحوسبة السحابية غير محمية بموجب أحكام القانون؛ كونه لم يفترض وجود مزودي خدمات سحابة مسؤولين عن حماية البيانات.
- ٢ - التعقييدات التقنية المرتبطة بهذا النوع من العقود تثير تحديات قانونية، خاصة تلك المرتبطة بحماية البيانات، وتحديد حقوق والتزامات كل طرف من أطراف العقد، في ظل تزايد حجم البيانات المتبادلة والمخزنة على السحابة، وظهور خوادم متعددة في دول عديدة لمزود خدمات.
- ٣ - الحوسبة السحابية خارج حدود الدولة السحب الخارجية تثير مخاوف بشأن فقدان التحكم بالبيانات ومشاركتها خارج نطاق العقد المستخدمين، وبالتالي تؤثر على مستخدمي تلك السحابات، كما أن القانون لم يوضح إذا كان الانتهاك من مسؤول أو معالج خارج حدود المملكة وأدى إلى فقدان التحكم بتلك البيانات.
- ٤ - عقود خدمات الحوسبة السحابية ليست عقود إذعان، ويحق للمستخدم أن يرفض التعاقد واللجوء إلى مزود خدمات سحابية آخر بالشروط التي يراها متلائمة مع نوع الخدمة التي يرغب في استخدامها والتفاوض على شروط الخدمة.
- ٥ - يُلزم القانون المسؤول والمعالج باتباع معايير صارمة لحماية البيانات، بما في ذلك تطبيق التدابير الأمنية ضد الانتهاكات والاختراقات.

- ٦ - التحديات الأمنية المتعلقة بحماية البيانات تظل قائمة خاصة في مواكبة التغيرات التقنية السريعة، وضمان الامتثال لأحكام القانون.

التوصيات

- ١ - تعديل قانون حماية البيانات الشخصية الأردني ليشمل أحكاماً خاصة تتعلق بخدمات الحوسبة السحابية، مع التركيز على مسؤوليات مزودي الخدمة السحابية، خصوصاً تلك التي تعمل خارج المملكة.
- ٢ - تحديد مسؤولية مزودي الخدمات في معالجة البيانات عبر الحدود، حيث ينبغي توضيح مسؤوليات مزودي خدمات الحوسبة السحابية بشأن معالجة البيانات الشخصية التي تنتقل عبر الحدود الدولية، وإضافة أحكام تضمن عدم نقل البيانات إلى دول لا تمتلك إطاراً قانونياً مماثلاً لحماية البيانات.
- ٣ - إنشاء آلية قانونية ورقابية تضمن التزام مزودي خدمات السحابة المحليين والدوليين بالمعايير القانونية لحماية البيانات الشخصية، بما في ذلك التزامهم بعدم نقل البيانات إلى خارج البلاد إلا بموجب عقود تضمن الحماية الكافية.
- ٤ - توفير أدوات تمكن المستخدمين من إدارة بياناتهم بسهولة، بما في ذلك مراقبة استخدام البيانات، واسترجاعها أو حذفها عند الطلب، بالإضافة إلى الإبلاغ الفوري عن أي اختراقات.
- ٥ - وضع تشريعات واضحة تنظم خدمات الحوسبة السحابية لتنظم الأمور القانونية التي غفل عنها قانون حماية البيانات الشخصية، وأهمية وجود تنسيق دولي لضمان حماية البيانات وحقوق الأفراد وفقاً للقواعد الدولية؛ كون عقد السحابة عقداً عابراً للحدود.
- ٧ - وضع اتفاقيات مع الدول التي تستضيف مراكز بيانات السحابة لتعزيز التعاون في حماية البيانات، وضمان الامتثال للقوانين المحلية والدولية.
- ٨ - تعزيز حقوق الأفراد في الوصول إلى البيانات، بحيث يجب أن يشمل القانون نصوصاً تنظم بشكل أوضح كيفية تقديم الأفراد لطلبات الوصول إلى بياناتهم المخزنة لدى مزودي الخدمات السحابية، وضمان الاستجابة لهذه الطلبات في فترات زمنية معقولة، مع عقوبات في حالة التأخير أو عدم الامتثال.

٩ - إلزامية التبليغ عن الاختراقات، بحيث يلزم مزودو الخدمات السحابية بإبلاغ الجهات التنظيمية والأفراد المعنيين بشكل فوري عند حدوث أي خرق أمني يؤثر على سلامة البيانات الشخصية، بما يضمن تقليل الأضرار الناتجة عن تلك الانتهاكات.

المراجع

- Mell. Peter, Grance. Timothy “The NIST Definition of Cloud Computing, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg” 2011, website <https://nist.gov>, visit date 25 Sep 2024.
- K.Nikhila, “Cloud computing” 2022 website <https://vardhaman.org/wp-content/uploads/2022/06/Cloud-Computing.pdf> 1 (1), visit date 14 Jul 2024.
- Buyya. Rajkumar, Broberg. James, Goscinski. Andrzej, “Cloud Computing” (John Wiley & Sons, Inc, USA, First Edition 2011).
- Simmon. Eric, “Evaluation of Cloud Computing Services Based on NIST SP 800-145” 2018 website <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf>.
- Pal. Souvik, Dac-Nhuong Le, Pattnai. Prasant Kumar, “Cloud Computing Solutions” (John Wiley & Sons, Inc, USA, First Edition 2022).
- Montgomery. Todd, Olson. Stephen, “Cloud Complete Study Guide” (John Wiley & Sons, Inc., Indianapolis, Indiana, USA, 2011).
- Fogarty. Vincent, Flucker. Sophia, “Data Centre Essential” (John Wiley & Sons Ltd, USA, First Edition 2023).
- P. Martin. James, Cendrowski. Harry, “Cloud Computing and Electronic Discovery” (by John Wiley & Sons, Inc, Hoboken, USA, Edition one 2014).
- Amazon, AWS Service Agreement, Website of Amazon <https://aws.amazon.com> visit date 20 Sep 2024.
- Hon. W. Kuan, Millard. Christopher, Walden. Ian, “Negotiating Cloud Contracts; Looking at Clouds from Both Sides Now” (2012) 16 Stanford Technology Law Review Journal

- Millard, Christopher, "Cloud Computing Law" (Oxford University, United Kingdom, British Library Cataloguing in Publication Data Second Edition 2021).
- Saeid .Abolfazli, L. Alcantara. Lailani and others, "Encyclopedia of Cloud Computing" (John Wiley & Sons, Ltd United Kingdom First Edition 2016).
- Cloud Act, Website www.justice.gov/d9/pages/attachments/2019/04/09/cloud_act.pdf (2018) visit date 5 Dec 2024.
- Zimmeck, Sebastian, "The Information Privacy Law of Web Applications and Cloud Computing" (2013) 29 Santa Clara Computer & High Technology Law Journal 451.
- وزارة الاقتصاد الرقمي والريادة الأردنية "سياسة المنصات السحابية وخدماتها" (وزارة الاقتصاد الرقمي والريادة، ٢٠٢٠). www.modee.gov.jo الدخول في ٢ / ٩ / ٢٠٢٤.
- الدستور رقم ١٠٩٣ لسنة ١٩٥٢ الدستور الأردني.
- القانون رقم ٤٣ لسنة ١٩٧٦ القانون المدني.
- قانون رقم ١٦ لسنة ٢٠١٩ الأمن السيبراني.
- قانون رقم ١٧ لسنة ٢٠٢٣ الجرائم الإلكترونية.
- قانون رقم ٢٤ لسنة ٢٠٢٤ حماية البيانات الشخصية.

The Issues of Independence and Dependence Between the Crime of Money Laundering and the Predicate Offense: A Comparative Study Between Kuwaiti and French Law

Dr. Lilian Alomyan*

Abstract:

Objectives: The study aims to identify the extent to which the Jordanian legislator protects data within the framework of the cloud computing services contract, by knowing the concept of cloud computing, its types, and the forms of providing cloud services due to the complexity of the technical function performed by cloud computing technologies represented in storing, preserving and processing data. The rights and obligations of both the cloud service provider and the user are not clear in terms of data. **Methodology:** The study used the analytical method as the method that suits the purpose and nature of the study, by reading the texts of the civil law regulating contracts and applying them to cloud computing services, dealing with data and processing data, and the rights and obligations of each party to the contract in cloud computing. **Results:** The results showed that while the Personal Data Protection Law establishes general provisions related to data protection, it does not explicitly address cloud computing as a means of storing and processing data. The study recommended the need to regulate cloud computing within the framework of data protection in Jordanian legislation, clarify the distribution of responsibilities between service providers and users, and develop provisions that reflect the technical reality of cloud environments. **Conclusion:** The study concluded on the need for Jordanian legislation to adequately protect data within the framework of cloud computing contracts.

Keywords: cloud computing, data, service provider, personal data protection.

* PhD of Law, Faculty of Law, University of Jordan..

Email: Lilian.Alomyan@ncsc.jo / LilianAlomyan@outlook.com

- Submitted: 28/10/2024, Accepted: 17/12/2024.

د. ليليان رياض إبراهيم العميان، مستشارة قانونية في المركز الوطني للأمن السيبراني الأردني، وباحثة قانونية في التشريعات المتعلقة بتكنولوجيا المعلومات والأمن السيبراني وحماية البيانات. حاصلة على درجة الدكتوراه في القانون من الجامعة الأردنية. ودرجة الماجستير في القانون- الجامعة الأردنية. التخصص الدقيق: تشريعات تكنولوجيا المعلومات والأمن السيبراني وحماية البيانات.

البريد الإلكتروني: Lilian.Alomyan@ncsc.jo / LilianAlomyan@outlook.com

للاستشهاد:

العميان، ليليان. (٢٠٢٦). مدى الحماية القانونية للبيانات الواردة في عقود خدمات الحوسبة السحابية؛ دراسة في القانون الأردني. مجلة الحقوق، جامعة الكويت، ٥٠ (١)، ٣٦٥-٣٢٩.

To Cite:

Alomyan, LiLian. (2026). The Extent of Legal Protection for Data Contained in Cloud Computing Services Contracts: A Study in Jordanian Law. *Journal of Law, Kuwait University*, 50(1), 329-365.

JOURNAL OF LAW

A Refereed Academic Quarterly, Published by the Academic Publication Council - University of Kuwait

The Issues of Independence and Dependence Between the Crime of Money Laundering and the Predicate Offense: A Comparative Study Between Kuwaiti and French Law

Dr. Lilian Alomyan



جامعة الكويت
KUWAIT UNIVERSITY

P-ISSN: 1029 - 6069

E-ISSN: 2960 - 2742

No. 1 - Vol. 50

Ramadan 1447 - March 2026