حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية

Protection of user's personal data in cloud computing contracts

بن لشهب أسماء *، كلية الحقوق، جامعة الإخوة منتوري – قسنطينة 1–

asma.benlecheheb@umc.edu.dz

تاريخ إرسال المقال: 07/ 02/ 2024 تاريخ قبول المقال: 30/ 04/ 2025 تاريخ نشر المقال: 13/ 05/ 2025

الملخص:

مع تسارع وتيرة التحول الرقمي احتلت الحوسبة السحابية مكانة هامة كمجال تكنولوجي متطوّر، يقدم خدمات متنوعة ومرنة تعتمد على شبكة الإنترنت من أهمها خدمة التخزين السحابي للبيانات، وعلى الرغم من المزايا العديدة التي توفرها هذه التكنولوجيا إلا أنها تحمل في طياتها عددا من المخاطر، لا سيما تلك المتعلقة بأمن وخصوصية البيانات الشخصية للمستخدم المخزنة سحابيا، حيث تتعرض هذه البيانات للاختراق والهجمات الإلكترونية المختلفة، وهو ما من شأنه المساس بالحق في حرمة الحياة الخاصة لمتلقي الخدمة السحابية. لهذا فقد حاولنا من خلال هذه الدراسة رصد أهم المخاطر التي تهدد الأمان في عقود الحوسبة السحابية، والتطرق إلى وسائل مواجهتها سواء من الناحية القانونية أو التقنية، وقد توصلنا إلى أن الحوسبة السحابية تشكل المستقبل في تخزين وإدارة البيانات إذا ما تم تبني مستويات أمان قوية لحماية البيانات الشخصية.

الكلمات المفتاحية: بيانات شخصية، حوسبة سحابية، أمان سحابي، حماية قانونية، حماية تقنية.

Abstract:

With the rapid digital transformation, cloud computing gained a significant position as a developed technological field providing varied and flexible services over the internet, most notably cloud storage of data. Despite its advantages, this technology presents many risks, namely those related to the security and privacy of users' personal data stored in the cloud. In fact, the stored data may be intercepted and subjected to different electronic attacks that violate cloud users' privacy. The present study aims to identify the major risks threatening security in cloud computing contracts and explore legal and technical methods to mitigate these risks. The results indicate that cloud computing represents the future of data storage and management if robust security measures are implemented to protect personal data.

Key words: personal data, cloud computing, cloud security, legal protection, technical protection.

* المؤلف المرسل

المقدمة:

لقد أدى التطور التكنولوجي المتسارع إلى اتجاه الأفراد والشركات على حد سواء نحو زيادة استخدام الحوسبة السحابية من أجل حفظ البيانات واستخدام التطبيقات على شبكة الإنترنت بدلا من الأجهزة الشخصية للمستخدمين، ويعود ذلك إلى ما تحققه هذه التكنولوجيا من فوائد، فمن خلالها تحولت البنية التحتية وبرامج تكنولوجيا المعلومات من مجرد منتجات تشترى إلى خدمات تقدم، وهو ما وفر على المستخدمين نفقات الحصول على البينة التحتية والبرامج اللازمة لتخزين وإدارة البيانات وتطوير هذه البرامج وصيانتها، ولم تعد الشركات بحاجة إلى البحث عن أكثر الحواسيب تطورا وأكبر الوحدات التخزينية سعة حتى تتمكن من الاحتفاظ بنسخ احتياطية عن بيانات عملائها، لكونها ستستفيد من مساحة التخزين الواسعة التي توفرها السحب الحاسوبية، وهو ما يمكنها من تحسين إدارة هذه البيانات وتعزيز كفاءتها التشغيلية، إذ مكنتها هذه التقنية من توسيع نطاق عملياتها بأقل تكلفة وأكبر جودة وهو ما يؤثر لا محالة على فعاليتها الإنتاجية.

إلا أن التوسع في استخدام تكنولوجيا الحوسبة السحابية مرهون بتوفير المتطلبات الأمنية اللازمة لحماية بيانات المستخدمين الشخصية المخزنة، وذلك بهدف تحقيق الثقة بين المستخدم ومقدم الخدمة، فالانتقال نحو بيئة الحوسبة السحابية ينطوي على عدة تحديات يشكل أمن البيانات الشخصية أهمها، فرغم أن الشركات المقدمة لخدمة التخزين السحابي تعمل على تشفير هذه البيانات قبل القيام بتخزينها إلا أن هذا لا يمنع من مهاجمتها واختراقها، وهو ما قد يؤدي إلى مخاطر كبيرة ومكلفة، وبهذا يلعب الأمان السحابي دورا مهما في الحفاظ على سرية وسلامة البيانات الشخصية في إطار عقود الحوسبة السحابية.

ولا يخفى علينا حجم الأهمية التي تحظى بها البيانات الشخصية في العصر الحديث، حيث أضحت نفط الثورة الصناعية الجديدة والمحرك الرئيسي للاقتصاد وحتى لنشوب الحروب في العالم وذلك من أجل السيطرة عليها والاستئثار بها، فمن خلال تحويل البيانات الشخصية إلى معلومات، وتحويل هذه المعلومات إلى معرفة يمكن فهم ميول الأشخاص والأسواق بهدف التحكم فيها، لهذا وبهدف ضمان سلامة وأمن وسرية هذه البيانات وكذلك خصوصيتها في إطار عقود الحوسبة السحابية، يمكننا طرح الإشكالية التالية:

هل الحماية القانونية والتقنية للبيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية كافية لضمان أمن وخصوصية هذه البيانات والحفاظ على سلامتها لا سيما في ظل التهديدات الأمنية التي تواجهها؟

للإجابة عن هذه الإشكالية ارتأينا الاعتماد على المنهج الوصفي بهدف الإحاطة بمفهوم كل من البيانات الشخصية والحوسبة السحابية وأهم التحديات الأمنية التي تواجههما، والمنهج التحليلي من خلال تحليل النصوص القانونية المتعلقة بحماية البيانات الشخصية.

وللإحاطة بهذا الموضوع فقد قسمنا دراستنا إلى قسمين، حيث تطرقنا لدراسة "مفهوم أمن البيانات الشخصية في إطار عقود الحوسبة السحابية"، ثم إلى "وسائل حماية البيانات الشخصية في إطار عقود الحوسبة السحابية".

1- مفهوم أمن البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية

إن استعمال الحوسبة السحابية لتخزين البيانات الشخصية للمستخدم قد يشكل خطرا على خصوصية هذه البيانات ويمس بمفهوم الأمان السحابي، ومن أجل توضيح ذلك سنتطرق أولا إلى مفهوم البيانات الشخصية للمستخدم التي قد تكون عرضة للاعتداء، ثم نحدد مفهوم عقود الحوسبة السحابية، لنتناول بعدها مفهوم الأمان في عقود الحوسبة السحابية.

1.1- مفهوم البيانات الشخصية:

إن البيانات الشخصية التقليدية لا تختلف عن نظيرتها الرقمية إلا من حيث كون هذه الأخيرة يتم استخدامها عند التعامل مع الوسائط الإلكترونية، على غرار تكنولوجيا الحوسبة السحابية، وحتى نتمكن من تحديد نطاق الحماية القانونية لهذه البيانات، يتعين تعريفها ثم توضيح أهم صورها.

1.1.1- تعريف البيانات الشخصية:

البيانات الشخصية التي قد تكون محلا للاعتداء عليها في إطار الحوسبة السحابية هي معلومات متعلقة بالشخص نفسه وتندرج في إطار طبيعته كإنسان، كاسمه وعنوانه ووضعه الصحي وعمره وجنسه وأصله العرقي وتوجهه الأخلاقي والسياسي[1]، كما تعرف كذلك بأنها معلومات مرتبطة بالشخص الطبيعي وتكون ملازمة له وتجعله معرفا أو قابلا للتعريف، وذلك أيا كان شكلها أو ما يميزها من خصائص، سواء كانت حرفية أو رقمية، ولو كانت في هيئة صورة أو في شكل ميزة صوت[2].

ولم يتفق التشريع والفقه المقارن على تسمية موحدة لهذه البيانات، فهناك من أطلق عليها مصطلح "البيانات الإسمية"، وهناك من أطلق عليها مصطلح "البيانات الشخصية"، وهي التسمية الأكثر تداولا، أما بالنسبة للمشرع الجزائري فقد استعمل مصطلح "المعطيات ذات الطابع الشخصي"، من خلال القانون 18-07[3] الذي يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة هذا النوع من المعطيات، وقد أورد في المادة 3 منه تعريفا لها بأنها معلومات أيا كانت دعامتها تتعلق بأشخاص معرفين أو قابلين لإمكانية التعرف عليهم، سواء كان ذلك بطريقة مباشرة أو بشكل غير مباشر، خاصة عن طريق الرجوع لرقم التعريف الخاص بهم أو العناصر الخاصة بهويتهم البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

وبدوره اتجه المشرع الفرنسي من خلال القانون رقم 78-17 المتعلق بالمعلوماتية والحريات عند تعديله سنة 2004[4] إلى تعريف البيانات الشخصية في المادة 2 منه بكونها معلومات تتعلق بأشخاص طبيعيين معرفين أو يمكن التعرف عليهم، سواء كان ذلك بكيفية مباشرة أو غير مباشرة، بالاستناد إلى رقم التعريف أو عنصر أو أكثر من العناصر الخاصة بهم[5].

من خلال ما تقدم يلاحظ أن التعريفات المقررة للبيانات الشخصية قد جاءت واسعة بحيث تنطبق على كل أنواع المعلومات طالما يمكن ربطها بشكل مباشر أو غير مباشر بالشخص الطبيعي، وذلك بغض النظر

عن طبيعتها أو قيمتها أو شكلها، فهذه البيانات لا يمكن حصرها فقد تتعلق بحياة الفرد الخاصة أو العامة أو المهنية، كما أن الحماية القانونية المقررة لهذه البيانات تقتصر على الشخص الطبيعي دون الشخص الاعتباري.

2.1.1- صور البيانات الشخصية:

تنقسم البيانات الشخصية المشمولة بالحماية في إطار القانون 18-07 إلى نوعين: فهناك **البيانات الشخصية العادية** وهي معلومات شخصية تسمح بتحديد هوية الشخص الطبيعي وتمييزه عن غيره، وقد تجعله قابلا للتعريف، ومن أمثلتها: الاسم واللقب، تاريخ الميلاد، رقم بطاقة التعريف، رقم الهاتف، عنوان البريد الإلكتروني...، وبما أن المشرع قد حصر قائمة البيانات الحساسة فما يخرج عنها من بيانات شخصية يعتبر بيانات عادية تخضع للحماية.

وهناك **البيانات الشخصية الحساسة**، وقد عرفها المشرع الجزائري في نص المادة 3 من القانون 18-07 بأنها معطيات تكتسي طابعا شخصيا وتظهر أصل الشخص المعني أو آرائه وقناعاته سواء كانت سياسية أو دينية أو فلسفية أو توضح انتماءاته النقابية، كما قد تتعلق بصحته بما فيها معطياته الجينية، من خلال هذا التعريف يلاحظ أن المشرع قد عرف البيانات الحساسة بحصر قائمة تشمل هذه البيانات، وعليه يخرج من هذه القائمة البيانات البيومترية وكذا البيانات المتعلقة بالتوجه الجنسي، كما نستحسن قيام المشرع بتعريف بعض المصطلحات التي جاءت في تعريف البيانات الحساسة في نص المادة 3 المذكورة على غرار المعطيات الجينية والمعطيات في مجال الصحة لإزالة الغموض عنها.

وعليه فالبيانات الحساسة هي عبارة عن بيانات يمكن أن ينتج عن معالجتها آثار وأضرار بالغة إذا ما قارناها بالبيانات العادية[6]، فقد تسمح معالجة هذه البيانات بالكشف عن أصل الفرد ومعتقداته وتوجهاته السياسية ومعلوماته الطبية، وهو ما يشكل خطورة ظاهرة على حياته الخاصة وحقوقه وحرياته الأساسية المحمية دوليا ودستوريا، لهذا السبب كرس المشرع الجزائري بشكل صريح في نص المادة 18 من القانون 18-07 حظر القيام بمعالجة المعطيات الحساسة، إلا أنه لم يجعل هذا الحظر مطلقا بل قرر عددا من الاستثناءات التي تجيز معالجة هذا النوع من البيانات، لكنه فرض قيودا ومتطلبات مشددة من أجل هذه المعالجة.

2.1 - مفهوم عقود الحوسبة السحابية:

لا تزال الحوسبة السحابية تحظى بجانب كبير من الغموض لدى عدد كبير من الأشخاص، ولبيان مفهومها سنتطرق إلى تعريفها وأهم مميزاتها وعيوبها.

1.2.1- تعريف عقد الحوسبة السحابية:

لقد تعددت العبارات المستخدمة لترجمة تكنولوجيا الـ "Cloud Computing" من أهمها: الحوسبة الافتراضية، الخادم الخاص الافتراضي، والحوسبة الإلكترونية، لكن عبارة الحوسبة السحابية تعد الأكثر تداولا في مجال تكنولوجيا المعلومات للتعبير عن (CC).

وتختلف التعريفات المقدمة للحوسبة السحابية حسب الزاوية التي ينظر منها إلى هذه التقنية، فالمختصون في علم الحاسوب يرون بأن الحوسبة السحابية هي: "تكنولوجيا تستغل قوة التخزين الهائلة للخوادم والتي تكون متباعدة ومتصلة ببعضها البعض عن طريق شبكة الإنترنت، والتي يتولى إدارتها مقدم الخدمة السحابية، وهذا ما يتيح للمستخدم الوصول إلى الموارد المخزنة في هذه الخوادم عن بعد من خلال استخدام جهاز طرفي موصول بشبكة الإنترنت (حاسوب، هاتف محمول، لوحة رقمية)"[7].

وبهذا يمكن القول أن الحوسبة السحابية هي تقنية تقوم على نقل القدرة التخزينية لجهاز الحاسوب الذي يملكه المستخدم إلى ما يطلق عليه بـ "السحابة"، وهذه الأخيرة هي عبارة عن أجهزة خوادم (servers) يمكن الوصول إليها من خلال شبكة الإنترنت، كما يقصد بها الوصول عبر شبكة الإنترنت –عند طلب المستخدم وبخدمة ذاتية– إلى البيانات والموارد الحاسوبية المخزنة على الخوادم.

وفي الجزائر يتولى تأطير نشاط استضافة خدمات الحوسبة السحابية دفتر شروط أعدته سلطة ضبط البريد والمواصلات السلكية واللاسلكية سنة 2017 (حاليا سلطة ضبط البريد والاتصالات الإلكترونية)، وقد أورد تعريفا لتكنولوجيا الحوسبة السحابية بكونها نموذج يسمح بالوصول من خلال الشبكة إلى عدد من الموارد المادية أو الافتراضية القابلة للزيادة والمتسمة بالمرونة والتي بالإمكان تزويدها وتسييرها عند الطلب وبالخدمة الذاتية[8]، ويخضع ممارسة نشاط تقديم خدمات الحوسبة السحابية إلى الحصول على ترخيص من طرف سلطة الضبط، ويمنح لمدة 5 سنوات قابلة للتجديد.

أما المختصون في المجال القانوني فينظرون إلى الحوسبة السحابية بأنها عقد يرتب التزامات متقابلة في ذمة طرفيه، ومن هذا المنطلق يعرف عقد الحوسبة السحابية (the contract of Cloud Computing) بأنه: "الاتفاق الذي يتبادل فيه المستخدم ومقدم الخدمة السحابية الإيجاب والقبول عبر شبكة اتصالات دولية إلكترونية ومفتوحة، وذلك بالاعتماد على نماذج معدة مسبقا ومعالجة إلكترونيا، وتنشأ عنه التزامات تعاقدية متقابلة من أجل الاستفادة من الأنظمة الحاسوبية التي يملكها مقدم الخدمة نظير التزام المستفيد بدفع مقابل مادي"[9].

من خلال هذا التعريف يلاحظ أن عقد الحوسبة السحابية يبرم بين شخصين أحدهما يسمى مقدم خدمة الحوسبة السحابية (cloud computing provider)، وهو شركة تقوم بتخزين بيانات وملفات عملائها وتزودهم بالبنية التحتية والوسائل المعلوماتية ليتمكنوا من الوصول إليها من خلال الإنترنت في أي زمان ومن أي مكان، أما الطرف الثاني فيتمثل في المستخدم (user) وهو الشخص الطبيعي أو المعنوي الذي يستفيد من

خدمات الحوسبة السحابية من خلال استئجار مساحة تخزينية على الخوادم المرتبطة بهذه الخدمة مقابل دفع مبلغ نقدي.

ونظرا لحداثة هذا العقد لم تضع غالبية التشريعات نصوصا خاصة لتنظيمه، وهو ما أدى إلى قيام اختلاف فقهي حول التكييف القانوني له، فهناك من اعتبر أن عقد تقديم خدمات الحوسبة السحابية هو عقد غير مسمى، وهناك من اعتبره عقد مقاولة باعتبار أن مقدم الخدمة السحابية يلتزم بأن يوفر خدمة إلكترونية للمستخدم (أداء عمل) مقابل قيام المستخدم بدفع أجر[10]، بينما هناك من يرى أن خدمة الحوسبة السحابية هي عقد إيجار يؤجر بمقتضاه مزود الخدمة مساحة تخزينية معينة على خوادمه لصالح المستخدم مقابل مبلغ من المال[11].

2.2.1- مزايا الحوسبة السحابية وعيوبها:

تحقق الحوسبة السحابية مزايا عديدة للمستخدمين سواء كانوا أفرادا أو مؤسسات، إلا أنها كأي تكنولوجيا حديثة تعتمد في عملها على شبكة الإنترنت لا تخلو من المساوئ والعيوب التي يمكن أن تحد من انتشار استخدامها، وتتمثل أهم مزايا وعيوب الحوسبة السحابية في[12]:

- المزايا:

- توفر الحوسبة السحابية على المستخدم تكاليف شراء أسرع أجهزة الحاسوب وأعلاها سعة تخزينية من أجل تخزين بياناته وعمل نسخ احتياطية عنها، حيث يمكنه الوصول إلى الخدمات السحابية المختلفة باستعمال جهاز حاسوب عادي ومتصفح للويب، ذلك أن الشركة المقدمة للخدمة تتحمل تكاليف البنية التحتية، إضافة إلى مصاريف صيانة وتطوير البرامج ومصاريف العمال الذين يديرون الخوادم، ويلتزم المستخدم فقط بدفع مقابل نظير السعة التخزينية التي يستهلكها.

- توفر خوادم الحوسبة السحابية مساحة تخزينية ضخمة للمستخدم، فلا حدود لتخزين بياناته ومعالجتها على السحابة على المستوى النظري، كما يمكن للمستخدم زيادة أو تقليل قدر احتياجاته التخزينية بسرعة ومع دفع مقابل لذلك.

- تعمل خدمة التخزين السحابي بشكل دائم على مدار الساعة، حيث يمكن للمستخدم الوصول إلى بياناته المخزنة على السحابة في أي وقت ومن أي مكان باستخدام الإنترنت، لأن بياناته مخزنة على خوادم الشركة وليس على حاسوبه الشخصي، وفي حالة وقوع أعطال طارئة تلتزم الشركة بإصلاحها في أسرع وقت.

- يساهم التوجه نحو استخدام تكنولوجيا الحوسبة السحابية في دعم مفهوم الحوسبة الخضراء، فمن جهة ستتخلص الشركات والمؤسسات من كمية كبيرة من الأجهزة المستهلكة للطاقة والتي تنبعث منها كميات من الغازات الضارة بالبيئة، كما سيتقلص حجم النفايات الإلكترونية بسبب قلة استخدام هذه الأجهزة من جهة أخرى.

- العيوب:

– يتطلب عمل تكنولوجيا الحوسبة السحابية الاتصال الدائم بشبكة الإنترنت، وبناء عليه إذا حصل مشكل في الاتصال أو عطل في الشبكة قد تتوقف الخدمات السحابية بشكل مؤقت أو كلي، وهو ما يمنع المستخدم من الوصول إلى بياناته وملفاته المخزنة على السحابة.

– إن المستخدم في عقود الحوسبة السحابية ينقل بياناته إلى السحابة التي يملكها مقدم الخدمة ويديرها بالكامل، فهو لا يتحكم ولا يدير البنية التحتية السحابية الأساسية وما تحتويه من شبكة وخوادم ونظم تشغيل وتخزين وغيرها، وذلك ما يؤدي بالضرورة إلى فقدانه السيطرة الحصرية على هذه البيانات ولا يصبح بإمكانه التأكد من مستويات الأمان المتخذة لحمايتها.

– تسمح تكنولوجيا الحوسبة السحابية بتخزين كم هائل من البيانات الشخصية على خوادم خارجية متصلة ببعضها عبر شبكة الإنترنت، وهذا ما يثير المخاوف حول أمن وخصوصية هذه البيانات، فقد تكون عرضة لمخاطر كبيرة وهجمات سيبيرانية كالوصول غير المصرح به للبيانات أو الكشف عنها أو إساءة استخدامها أو قرصنتها، ويمكن رد أسباب النفاذ إلى البيانات المخزنة سحابيا إلى الافتقار إلى إدارة للوصول إلى الهوية، ونقص الرؤية والضوابط ووسائل التحكم، وضعف في تكوين السحابة.

3.1– مفهوم الأمان في عقود الحوسبة السحابية:

يلعب الأمان السحابي دورا مهما في الحفاظ على سرية وسلامة البيانات الشخصية في إطار عقود الحوسبة السحابية، ولتوضيح ذلك سنتطرق إلى تعريف الأمان السحابي، وبعدها ننتقل إلى رصد المخاطر التي تهدد الأمان في عقود الحوسبة السحابية.

1.3.1– تعريف الأمان السحابي:

يعتبر أمن المعلومات (Information Security) أحد فروع العلوم التقنية الحديثة، وهو علم يختص بتوفير الحماية اللازمة للمعلومات والبيانات المتداولة من خلال شبكة الإنترنت والمحفوظة بشكل رقمي من المخاطر التي تهددها، عن طريق تبني ممارسات أو استخدام وسائل تحميها من التهديدات الداخلية والخارجية، سواء تعلق الأمر بالوصول غير المصرح به للبيانات أو تعديلها أو سوء استخدامها أو تعطيلها أو تدميرها أو سرقتها[13].

وقد حددت المادة 1 من القانون المصري المتعلق بحماية البيانات الشخصية رقم 151 لسنة 2020 المقصود بأمن البيانات بكونه عبارة عن مجموعة من العمليات والإجراءات التقنية والتنظيمية التي تسمح بالمحافظة على خصوصية البيانات الشخصية وسريتها وسلامتها ووحدتها وكذلك تحفظ تكامل هذه البيانات فيما بينها[14].

ومن هذا المنطلق يقصد بأمان الحوسبة السحابية (Cloud Computing Security) أو ما يطلق عليه "الأمان السحابي" مجموعة من التدابير والسياسات والتكنولوجيات التي تستخدم لتأمين تطبيقات الحوسبة السحابية وبنيتها التحتية، والمحافظة على أمن وخصوصية البيانات الشخصية المحفوظة فيها.

وينقسم أمن البيانات الإلكترونية في إطار عقود الحوسبة السحابية إلى قسمين، يتمثل الأول في الأمن الداخلي للسحابة وهدفه حماية بيانات المستخدم المخزنة فيها وعزلها عن العالم الخارجي، فلا يسمح بالولوج إليها إلا للمستخدم الذي يكون دخوله إلى السحابة خاضعا للرقابة ومقتصرا على بياناته المخزنة دون بيانات المستخدمين الآخرين، أما الأمن الخارجي فهدفه حماية هذه البيانات عند انتقالها من السحابة وإليها[15].

وتتبع معظم الشركات المقدمة للخدمات السحابية نموذج المسؤولية المشتركة، وهو ما يقصد به أن تحقيق أمان الحوسبة السحابية يقع على كل من مزود الخدمة والمستخدم، فمقدم الخدمة مسؤول بشكل عام عن السحابة وبنيتها الأساسية وهو ملزم بحفظ بيانات العميل الشخصية وعدم فقدانها، والمستخدم بدوره ملزم بالتأكد من التخزين الفعلي لبياناته وتأمين عناصر التحكم في الشبكة والهوية من خلال المحافظة على سرية معلومات الاتصال وعدم الإفصاح عنها للغير[16]، لكن وفي الآونة الأخيرة، ظهر نموذج جديد لأمن الحوسبة السحابية والذي تحولت بموجبه المسؤولية المشتركة إلى نموذج المصير المشترك، وفي ظل هذا النموذج يوفر مزود الخدمة السحابية إرشادات وموارد وأدوات أكثر شمولا لمساعدة العملاء على الحفاظ على الاستخدام الآمن للسحابة، بدلا من ترك العملاء يتنقلون بين إدارة المخاطر في البيئات السحابية الأصلية.

وتجدر الإشارة إلى أنه إذا كانت استراتيجية الأمان التي يتبعها مزود الخدمة السحابية قوية ومصممة بمعايير عالية فيمكنها الصمود طويلا أمام الانتهاكات والاختراقات التي تتعرض لها البيانات الشخصية أو على الأقل التخفيف من أضرار هذه الاعتداءات، كما أنها ستعمل على تدعيم ثقة العملاء، ومع ذلك مهما بلغت درجة الأمان السحابي فلا يمكنها أن تضمن بشكل مطلق حماية البيانات الشخصية ضد مخاطر الهجمات السيبيرانية.

2.3.1- المخاطر التي تهدد الأمان في عقود الحوسبة السحابية:

سبق القول أن التخزين السحابي للبيانات يقدم العديد من المزايا لكنه في المقابل لا يخلو من المخاطر، لكونه يعتمد بشكل أساسي على مزود خدمة خارجي يعتمد في عمله على شبكة الإنترنت ولديه السيطرة الكاملة على السحابة والبيانات المخزنة عليها، لهذا تعاني السحابة من مخاطر أمنية عديدة، فقد تتعرض البيانات الشخصية إلى هجمات من مصادر مختلفة، فمن جهة قد يقع الهجوم على هذه البيانات من طرف الأشخاص العاملين على تقديم الخدمات السحابية، فباعتبارهم يملكون الصلاحية للوصول إلى البيانات على السحابة، قد يعملون على إفشاء كلمة المرور أو المعلومات الخاصة التي يستعملها المستخدم بهدف الوصول إلى هذه البيانات لأشخاص آخرين أو مساعدة القراصنة على اختراق البيانات وتسريبها، كما قد يتعمدون القيام بحذف جزء من البيانات لتوفير مساحة تخزينية أكثر[17].

ومن جهة أخرى قد يكون الهجوم على السحابة من طرف خارجي عن طريق شبكة الإنترنت، كالاستيلاء على كلمات المرور ومعلومات المصادقة المتعلقة بالمستخدمين المعتمدين سواء باستعمال برامج التجسس أو باستعمال طريقة التصيد الاحتيالي (phishing)[18]، كما يستعمل القراصنة هجمات حجب الخدمة (DDoS)،

بالقيام بإرسال عدد كبير من الطلبات في آن واحد إلى مقدم الخدمة السحابية، من أجل تجاوز حدود طاقته على التعامل مع هذه الطلبات ومعالجتها، وهو ما يؤدي إلى توقف وتعطل البنية التحتية للسحابة عن العمل، وإضافة إلى ذلك يمكن للمعتدي استعمال برامج الابتزاز أو الفدية الضارة (Ransomwar)، من خلال قيام القراصنة بتهديد مزود الخدمة بتدمير البيانات الشخصية للمستخدمين التي يتولى تخزينها أو منع الوصول إليها حتى يقوم بدفع المال (الفدية)، سواء عن طريق استعمال برامج تتولى تشفير الملفات التي تخزن فيها البيانات (crypto)، حيث لا يمكن الوصول إليها حتى يدفع المال وعندها فقط يحصل الضحية على مفتاح فك التشفير، وهناك برامج تعمل على غلق الملفات (locker) بحيث تجعل الضحية غير قادر على تسجيل دخوله إلى البيانات حتى يدفع الفدية[19]، كما يمكن للقراصنة إرسال فيروسات لتدمير وإتلاف خوادم الحوسبة السحابية التي تخزن فيها البيانات الشخصية للمستخدمين، وهو ما قد يؤدي إلى فقدان هذه البيانات، لهذا تبدو أهمية إعداد نسخ احتياطية عنها تخزن بصفة مستقلة عن البيانات الأصلية.

وأيا كانت طريقة الاعتداء التي تتعرض لها البيانات الشخصية على السحابة فإنها تؤدي إلى مخاطر كبيرة، فهذه البيانات تسمح بإعطاء صورة متكاملة عن الشخص تكاد تكون أقرب للحقيقة، لهذا فإن الوصول غير المصرح به للبيانات الشخصية سيفقدها خصوصيتها، كما قد يؤدي الاعتداء إلى تسريبها أو فقدانها، وهو ما يفتح المجال لقيام المسؤولية القانونية للمعتدي ولمزود الخدمة السحابية.

2- وسائل حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية

تتنوع وسائل حماية البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية، بين الحماية القانونية بشقيها المدنية والجزائية، وكذا الحماية التقنية التي تلعب دورا كبيرا في الوقاية من وقوع الاعتداء على هذه البيانات أو التخفيف من آثاره إن كان قد وقع، وهو ما سنتطرق له فيما يلي:

1.2- الحماية المدنية:

إن الاعتداء على البيانات الشخصية للمستخدم في إطار عقود الحوسبة السحابية قد يلحق أضرارا بالغة به، وهو ما يسمح له برفع الدعوى المدنية للحصول على التعويض، وفي هذا الخصوص قد تثور إما المسؤولية العقدية للمسؤول عن الاعتداء كما يمكن أن تثور مسؤوليته التقصيرية، وهو ما سيأتي توضيحه فيما يلي:

1.1.2- دعوى المسؤولية العقدية:

إن عقد الحوسبة السحابية المبرم بين مزود الخدمة السحابية والمستخدم هو عقد ملزم لجانبين، حيث يرتب على عاتق المزود التزاما بتأجير مساحة تخزينية على خوادمه لبيانات المستخدم وتمكينه من الوصول إليها في أي وقت نظير قيام هذا الأخير بدفع مقابل نقدي، ويتفرع عن هذا الالتزام الرئيسي لمقدم الخدمة السحابية عدة التزامات أخرى من أهمها التزامه بعدم إفشاء البيانات الشخصية للمستخدم إلا في الحالات التي يسمح بها القانون، وكذا التزامه بتوفير الحماية الكافية لهذه البيانات وضمان أمنها وسلامتها، ومنع الغير من الاطلاع عليها أو انتهاك خصوصيتها، وعليه إذا أخل مقدم الخدمة بهذه الالتزامات وتعرضت البيانات الشخصية

للمستخدم للاختراق مما أدى إلى تلفها أو فقدانها أو تغييرها أو إفشائها قامت المسؤولية العقدية في جانب مقدم الخدمة، وأصبح بالتالي ملزما بدفع التعويض المستحق للمستخدم عن الضرر الذي أصابه[20].

والملاحظ أن غالبية مقدمي خدمة الحوسبة السحابية يستعملون عقودا نموذجية جاهزة معدة بشكل مسبق وموجهة إلى كافة الجمهور ولا تقبل بصفة مطلقة التفاوض فيها، حيث يخضع الولوج إلى خدمات السحابة إلى توقيع المستخدم على اتفاق إطار ولا يملك إلا قبول الشروط الواردة فيه أو رفضها، ومن هذا المنطلق يتجه مقدمو الخدمة في كثير من الأحيان إلى تضمين هذه العقود شروطا تفضي إلى تحديد مسؤوليتهم وحصر نطاقها في أنواع معينة من الأضرار، وهو ما دفع إلى اعتبار عقود الحوسبة السحابية عقود إذعان[21].

فإذا كان المبدأ أن يلتزم مقدم الخدمة السحابية بشكل كامل بالحفاظ على سلامة البيانات الشخصية وتكاملها، إلا أن الواقع يشير إلى أن مزودي الخدمة يختلفون في مستويات الحماية المقدمة للعميل، فهناك من يستعمل في العقد النموذجي عبارة "الالتزام ببذل أقصى جهد"، وهو ما يستشف منه أن التزام مقدم الخدمة في هذه الحالة يقتصر على بذله للعناية الواجبة لحماية البيانات الشخصية دون أن يلتزم بالوصول إلى تحقيق هذه الغاية، وهو ما سلكته مثلا كل من شركتي Microsoft وAmazon، وهناك شركات أخرى تطلب من المستخدم أن يدفع رسوما إضافية حتى تضمن له حماية بياناته الشخصية مثل شركة Rackspace[22].

وعليه يعتبر مقدم الخدمة السحابية أمينا على البيانات الشخصية لمتلقي الخدمة بموجب العقد المبرم بينهما، فهو ملزم بتوفير الحماية لها بما خوله له القانون من سلطات، فإذا لم يتخذ الإجراءات التقنية المناسبة والفعالة في هذا الشأن عُدّ مخطئا وقامت مسؤوليته العقدية، ولابد أن تضمن هذه الإجراءات قدرا ملائما من السلامة، مع الأخذ بعين الاعتبار طبيعة البيانات الشخصية الواجب حمايتها والمخاطر التي قد تتعرض لها، وكذا التقنيات المتاحة فيما يتعلق بحماية هذه البيانات[23].

وإضافة إلى ما سبق ذكره يمكن أن يتضمن عقد الحوسبة السحابية اتفاقا لمعالجة البيانات الشخصية التي أدلى بها المستخدم المتعاقد عند إبرام العقد، وفي هذا الصدد يتعين توضيح نوع البيانات محل المعالجة وطبيعة المعالجة والغرض منها والمرسل إليهم، ويجب الحصول على الموافقة الصريحة للمستخدم قبل القيام بمعالجة بياناته، كما لا يمكن إطلاع الغير عليها إلا لغايات محددة وبعد الموافقة المسبقة لصاحب البيانات[24].

كما أن مزود الخدمة السحابية المسؤول على المعالجة ملزم بأن تعالج البيانات الشخصية بكيفية مشروعة ونزيهة، وأن تكون مجمعة لغايات واضحة ومحددة، وأن تكون ملائمة وغير مبالغ فيها بالنسبة للغاية التي جمعت وعولجت بشأنها، وعليه كذلك أن يضمن حفظها بطريقة تسمح بالتعرف على مستخدم الخدمة السحابية في مدة لا تتعدى تلك الضرورية لتحقيق الغايات التي بشأنها تم جمعها ومعالجتها[25]، أما إذا قام مزود الخدمة السحابية بجمع البيانات الشخصية في شبكة مفتوحة، فيتعين عليه أن يعلم المستخدم أن بياناته قد يتم تداولها في الشبكة دون ضمان سلامتها وقد تكون عرضة لقراءتها واستعمالها بطريقة غير مرخصة من قبل الغير، هذا ما لم يكن يعلم بذلك سابقا[26].

ونظرا لرواج تجارة البيانات الشخصية وارتفاع المكاسب التي تحققها، فقد يقوم مزود الخدمة السحابية باستعمال البيانات الشخصية للمستخدمين لأغراض تجارية، على غرار بيعها لشركات التسويق والإعلان حتى تكيف منتجاتها وموادها الإعلانية مع رغبات المستهلكين واحتياجاتهم وتتمكن من اختيار الفئات المستهدفة، فقد منحت المادة 36 من القانون 18-07 المذكور سابقا لصاحب البيانات الحق في الاعتراض على استخدام بياناته لأغراض الدعاية، خاصة إذا كانت تجارية، وذلك ما لم تكن معالجة هذه البيانات استجابة لالتزام قانوني، أو تطبيقا للأحكام الواردة في عقد الحوسبة السحابية.

انطلاقا مما سبق إذا قام مزود الخدمات السحابية بجمع البيانات الشخصية دون موافقة المستخدم، أو إذا لم يحترم الالتزامات المتعلقة بمعالجة هذه البيانات في حالة ما إذا تضمن عقد الحوسبة السحابية اتفاقا بشأن هذه المعالجة، قام الخطأ في جانبه والتزم بتعويض المستخدم عن الأضرار اللاحقة به على أساس المسؤولية العقدية.

2.1.2- دعوى المسؤولية التقصيرية:

إن مساءلة مقدم الخدمة السحابية عقديا عند مخالفته لالتزامه بضمان حماية البيانات الشخصية للمستخدم لا تمنع من قيام المسؤولية المدنية لمرتكب الاعتداء، ولعدم وجود عقد يربط بين المعتدي ومتلقي الخدمة السحابية تطبق القاعدة العامة في المسؤولية التقصيرية المكرسة بموجب المادة 124 من (ق. م. ج)[27] التي تقرر بأن كل شخص ارتكب خطئا يسبب ضررا للغير يكون ملزما بتعويض هذا الضرر، فإذا قام شخص باختراق السحابة والوصول إلى البيانات الشخصية للمستخدم أو العبث فيها أو إتلافها أو إفشائها، كان مسؤولا عن تعويض الضرر المادي والمعنوي اللاحق بصاحب البيانات والناتج عن انتهاك حرمة حياته الخاصة التي كفلت حمايتها نصوص الاعلانات والاتفاقيات الدولية والدساتير والتشريعات الوطنية.

ويشترط لقيام المسؤولية التقصيرية أن يكون الضرر الذي لحق بالمستخدم قد وقع بشكل فعلي أو أن يتأكد وقوعه مستقبلا، أما إذا كان الضرر احتماليا فلا تعويض عنه، وعليه إذا استعمل المخترق فيروسا لا يفعل إلا في حالة قيام مستخدم الحوسبة السحابية بفتح الملف الذي يحوي بياناته الشخصية، فلا يعتبر ضررا مستقبليا مؤكد الوقوع، لأن المستخدم قد يزيل هذا الملف الذي التصق به الفيروس أو لا يفتحه مطلقا[28].

وفي حالة وقوع الاعتداء من الغير وكان التزام مقدم الخدمة هو التزام ببذل عناية يتعين التأكد من أن الشركة لم تقصر في أداء التزاماتها، فإذا ثبت ذلك فهناك من يرى بأنها لا تتحمل المسؤولية إلا إذا طبقت نظرية المخاطر المقابلة للربح، فما دام أنها تجني فوائد من تخزين بيانات المستخدمين فإنها تتحمل مخاطر ممارسة هذا النشاط[29].

أما إذا كان الهجوم على البيانات الشخصية داخليا من خلال قيام الأشخاص العاملين لدى مقدم الخدمة السحابية بالسماح لأشخاص غير مؤهلين بالولوج إلى البيانات الشخصية للمستخدم أو إفشاء هذه البيانات، فيمكن مساءلة مزود الخدمة السحابية على أساس المسؤولية التقصيرية للمتبوع عن فعل التابع إذا توفرت

شروطها الواردة في المادة 136 من (ق. م. ج)، إضافة إلى إمكانية مساءلتهم شخصيا باعتبارهم ملزمين إذا كانت البيانات الشخصية محل معالجة بالمحافظة على السر المهني سواء أثناء ممارسة مهامهم وكذا بعد انتهاء هذه المهام[30].

وأخيرا تجدر الإشارة إلى أن إخلال مزود الخدمة السحابية بالتزاماته المتعلقة بمعالجة البيانات الشخصية للمستخدم، إضافة إلى أنه يشكل إخلالا بالتزام عقدي فهو يعتبر جريمة معاقب عليها جزائيا بموجب نصوص القانون 18-07، لهذا يرى جانب من الفقه أنه يجوز للمضرور الخيرة بين المسؤوليتين العقدية والتقصيرية في هذه الحالة التي يشكل فيها الإخلال بالالتزام العقدي جريمة جنائية، لأنه إذا وصل الأمر بالمتعاقد إلى أن يرتكب جريمة يخرج بها عن الإطار العقدي، فلابد أن تتاح للمضرور ملاحقته بكل الوسائل القانونية المتاحة[31].

2.2- الحماية الجزائية:

لقد دعم المشرع الجزائري الحماية المدنية المقررة للبيانات الشخصية من الاعتداءات التي تطالها في إطار عقود الحوسبة السحابية، بالحماية الجزائية التي تهدف إلى ردع ومعاقبة المعتدي، ويظهر ذلك أساسا من خلال جريمة الدخول بطريقة غير مشروعة إلى نظام الحوسبة السحابية أو البقاء غير المشروع في هذا النظام، وكذا من خلال الجرائم المتعلقة بالمعالجة الآلية للبيانات الشخصية.

1.2.2- جريمة الدخول أو البقاء بطريقة غير مشروعة في نظام الحوسبة السحابية:

قد يتعرض النظام المعلوماتي لتكنولوجيا الحوسبة السحابية للاختراق من طرف أشخاص غير مصرح لهم بالدخول أو ما يطلق عليهم "القراصنة"، ونظرا لخطورة هذا السلوك الإجرامي على البيانات الشخصية للمستخدمين فقد قرر المشرع الجزائري في نص المادة 1/394 مكرر من (ق. ع. ج)[32] عقوبة المعتدي الذي يدخل أو يبقى في النظام المعلوماتي بطريق الغش بالحبس لمدة تتراوح من 3 أشهر كحد أدنى إلى سنة كحد أقصى، إضافة إلى العقوبة المالية المتمثلة في الغرامة المقدرة من 50 ألف د. ج إلى 100 ألف د. ج.

وبهذا تقوم هذه الجريمة عن طريق التسلل باستعمال الوسائل التقنية إلى نظام الحوسبة السحابية، وتتحقق بمجرد قيام المعتدي بالدخول إلى هذا النظام دون تصريح أو رخصة، وذلك تحقيقا لغايات مختلفة، فقد يكون هدف المخترق هو البيانات الشخصية المخزنة على السحابة فيقوم بتغييرها أو سرقتها أو إزالتها، وقد يكون هدفه هو النظام المعلوماتي بحد ذاته كأن يثبت ما يتمتع به من قدرات اختراقية أو حتى يثبت وجود ثغرات أمنية في هذا النظام[33].

وتختلف جريمة الدخول غير المشروع إلى نظام الحوسبة السحابية على جريمة البقاء داخل هذا النظام مع أن المشرع الجزائري قد جمعهما في نص تجريمي واحد ووحد العقوبة المقررة لهما، ففعل البقاء يقصد به التواجد داخل النظام ضد إرادة المسؤول عنه، وعلى الرغم من أن هذه الجريمة تكون عادة لاحقة لجريمة الدخول غير المشروع، إلا أنها قد تكون أحيانا مستقلة عنها، وتتحقق هذه الفرضية كأن يلج الشخص إلى نظام الحوسبة

السحابية بطريق الصدفة أو عن طريق الخطأ فينتهز الفرصة ويقرر البقاء في النظام ولا يفصل الاتصال ويخرج منه[34].

وسواء تعلق الأمر بجريمة الدخول غير المشروع أو جريمة البقاء غير المشروع في نظام الحوسبة السحابية فلا تقوم الجريمة حتى يتوفر القصد الجنائي لدى الجاني بعنصريه العلم والإرادة باعتبارها جريمة عمدية[35]، وهو ما يظهر من خلال استعمال المشرع الجزائري لعبارة "**بطريق الغش**" في نص المادة 1/394 مكرر المذكورة، كما يلاحظ أن هذه الجريمة هي جريمة شكلية تقوم بمجرد تحقق فعل الدخول أو البقاء غير المشروع، حيث لا يشترط أن يصل المخترق إلى البيانات الشخصية المخزنة في منظومة الحوسبة السحابية أو أن يلحق الضرر بالمستخدم صاحب البيانات، لكن إذا ما إذا أفضى الاختراق إلى تغيير أو حذف البيانات الشخصية المخزنة على هذا النظام فقد قرر المشرع مضاعفة العقوبة الواردة في المادة 1/394 مكرر من (ق.ع. ج) المذكورة أعلاه[36]، أما إذا قام المعتدي عمدا وبطريق الغش بحيازة البيانات المحصل عليها من هذه الجريمة أو إفشائها أو نشرها أو استعمالها أيا كان الغرض من ذلك، فقد سلط عليه المشرع عقوبة سالبة للحرية تتمثل في الحبس من شهرين كحد أدنى إلى 3 سنوات كحد أقصى، وكذلك الغرامة من 1 مليون د. ج إلى 5 مليون د. ج حسب نص المادة 394 مكرر 2 من (ق. ع. ج).

2.2.2-الجرائم المتعلقة بالمعالجة الآلية للبيانات الشخصية:

سبق القول أن عقد الحوسبة السحابية يمكن أن يتضمن اتفاقا بشأن المعالجة الآلية للبيانات الشخصية التي أدلى بها المستخدم عند إبرام العقد، وفي هذه الحالة يقع على مقدم الخدمة السحابية مجموعة من الالتزامات سبق ذكرها، وفي حالة مخالفته لذلك تتم مساءلته طبقا لنصوص القانون 18-07 الذي يهدف إلى حماية المعطيات الشخصية للشخص الطبيعي عند معالجتها آليا والمذكور سابقا، فإذا قام مزود الخدمة بجمع البيانات الشخصية دون الحصول على الموافقة الصريحة للشخص المعني تطبق عليه عقوبة الحبس لمدة تتراوح من سنة كحد أدنى إلى 3 سنوات كحد أقصى، وغرامة مالية من 100 ألف د.ج إلى 300 ألف د. ج حسب المادة 55 من هذا القانون، ونفس العقوبة تطبق إذا قام بالمعالجة رغم معارضة المستخدم خاصة إذا كان الهدف منها الإشهار التجاري، أو إذا كان اعتراض المستخدم مؤسسا على أسباب شرعية.

أما إذا تعلق الأمر بمعالجة البيانات الشخصية الحساسة لمتلقي الخدمة السحابية دون الحصول موافقته وخارج إطار الحالات المذكورة في القانون 18-07 فقد سلط المشرع الجزائري على مقدم الخدمة عقوبة الحبس لمدة تتراوح من سنتين كحد أدنى إلى 5 سنوات كحد أقصى، إضافة إلى دفع غرامة مالية من 200 ألف د. ج إلى 500 ألف د.ج حسب ما قررته المادة 57 من هذا القانون، بينما لو قام بإنجاز معالجة البيانات الشخصية أو استعمالها لأغراض مختلفة عن تلك المصرح بها أو المرخص لها فيعاقب طبقا للمادة 58 بالحبس من 6 أشهر إلى سنة إضافة إلى دفع الغرامة المالية من 60 ألف د.ج إلى 100 ألف د.ج، أو بواحدة فقط من هاتين العقوبتين، كما يعاقب من يسمح لشخص غير مؤهل بالولوج إلى البيانات الشخصية بالحبس كعقوبة

سالبة للحرية لمدة تتراوح من سنتين إلى 5 سنوات وبالغرامة المالية من 200 ألف د.ج إلى 500 ألف د.ج وفق المادة 60 من نفس القانون.

وإذا لم يقم مقدم الخدمة السحابية بوضع التدابير الملائمة لحماية البيانات الشخصية من إتلافها أو ضياعها أو تلفها أو النشر أو الولوج غير المرخصين تطبق عليه الغرامة كعقوبة مالية تتراوح من 200 ألف د.ج إلى 500 ألف د.ج، وتطبق نفس العقوبة إذا احتفظ بهذه البيانات متجاوزا المدة المنصوص عليها قانونا أو المحددة في التصريح أو الترخيص طبقا للمادة 65 من القانون 18-07، وإذا كان مقدم الخدمة الحسابية شخصا معنويا وارتكب إحدى الجرائم المنصوص عليها في هذا القانون فيعاقب طبقا للقواعد المنصوص عليها في قانون العقوبات حسب ما جاء في المادة 70 من القانون 18-07.

وقد قرر المشرع الجزائري تطبيق نفس العقوبة المقررة للجريمة التامة على محاولة ارتكاب إحدى الجنح المذكورة، وفي حالة العود تضاعف العقوبات المذكورة سابقا[37].

3.2- الحماية التقنية:

إن إعمال الحماية القانونية للبيانات الشخصية لمستخدم الحوسبة السحابية تواجهه عدة تحديات تحد من فعاليتها من أهمها: صعوبة تحديد هوية المعتدي، صعوبة إثبات الجريمة في ظل العالم الافتراضي لشبكة الإنترنت، الصعوبة المتعلقة بتحديد المحكمة المختصة والقانون الواجب تطبيقه على النزاع، صعوبة تنفيذ العقوبة إذا كان المعتدي يقيم بالخارج، الصعوبة المتعلقة بالتعاون القضائي الدولي في هذا الخصوص...[38]، هذا ما فرض حتمية التوجه نحو تبني وسائل حماية تتلاءم مع الطبيعة التقنية لنظام الحوسبة السحابية وشبكة الإنترنت باعتبارها البيئة التي تعمل فيها، وذلك لمنع وقوع الاعتداء أو على الأقل التخفيف من أضراره إن كان قد وقع، ومن أهم هذه الوسائل:

1.3.2- التشفير (encryption): وهو عملية يتم من خلالها تحويل البيانات الشخصية للمستخدم إلى رموز غير مفهومة عن طريق استخدام خوارزميات رياضية، وذلك بهدف حمايتها من الوصول غير المصرح به وضمان سلامتها وخصوصيتها سواء في مرحلة تخزينها أو نقلها، وبالتالي حتى لو تمكن المخترق من الوصول إليها فلن يستطيع قراءتها لكونه لا يملك مفتاح فك تشفيرها[39]، ويتم التشفير في إطار التخزين السحابي على مستويين: فقد يتم من طرف **المستخدم** من خلال قيامه بتشفير بياناته الشخصية قبل نقلها من جهازه وتحميلها على السحابة مستعملا مفتاحا يملكه هو فحسب، كما يمكن أن يتم التشفير من طرف **الخادم**، وذلك من خلال تشفير البيانات الشخصية بعد عملية تحميلها على السحابة من خلال استعمال مفتاح يديره مزود الخدمة السحابية، وهو ما يوفر الحماية لهذه البيانات أثناء تخزينها سحابيا.

ومن أحدث خوارزميات التشفير Honey encryption (HE) أو ما يطلق عليه "تشفير العسل"، والذي يستعمل عند تنفيذ المعتدي لهجوم "القوة الغاشمة" Brute-Force Attack، وهذا الأخير هو هجوم سيبيراني يقوم على تكرار المحاولة والتخمين والتجريب المنهجي لكل المجموعات الممكنة من أجل كسر كلمات المرور

أو مفتاح فك التشفير للوصول إلى النظام المعلوماتي للحوسبة السحابية أو البيانات المشفرة المحمية، حيث تستخدم تقنية (HE) كلمة المرور الأصلية وتنتج قائمة من كلمات المرور التي تشبهها إلى حد كبير، وعند محاولة المخترق فك تشفير البيانات الشخصية للمستخدم تمكنه كلمة المرور المزيفة من الدخول إلى حساب مزيف وبيانات مزيفة، وفي هذا الوقت يتم تنبيه المستخدم صاحب الحساب الأصلي بإرسال رسالة عاجلة حتى يتخذ الإجراءات المطلوبة، وهكذا يوهم تشفير العسل المخترق أنه حقق نجاحا كبيرا لكن ذلك لم يتحقق على أرض الواقع[40].

2.3.2- الجدار الناري (fire wall): هو نظام أمان يقوم على مراقبة حركة عبور البيانات من وإلى السحابة والتحكم فيها اعتمادا على سياسات أمان محددة سلفا، بهدف منع الاختراق والتسلل للبنية التحتية السحابية، وحماية البيانات الشخصية للمستخدم من الوصول غير المصرح به والهجمات السيبيرانية المختلفة، وذلك من خلال فلترة وتحليل تدفق البيانات إلى هذا النظام عن طريق الخوادم الوسيطة أو ما يسمى بالخادم الوكيل (proxy server)، الذي يعتبر بمثابة حاجز بين النظام المعلوماتي للحوسبة السحابية وشبكة الإنترنت، ويعمل على عزل هذا النظام كجدار ناري وهو ما يساعد على حمايته من أي اعتداء خارجي[41].

الخاتمة:

من خلال هذه الدراسة اتضح لنا أن تبني تكنولوجيا الحوسبة السحابية قد أضحى ضرورة لا غنى عنها تمليها متطلبات الوقت الحالي نتيجة الزيادة المتسارعة في حجم البيانات، وبالتالي الحاجة إلى مساحات تخزينية كبيرة تتجاوز القدرة الاستيعابية للأجهزة والبنية التحتية التي يملكها الأفراد والمؤسسات، لكن هذه التكنولوجيا بقدر ما وفرته من مزايا وخدمات بقدر ما أفرزته من مخاطر، لا سيما تلك المتعلقة بأمن البيانات الشخصية للمستخدمين المخزنة سحابيا، ومما لا شك فيه أن هذه البيانات تعد من قبيل الخصوصية المعلوماتية التي لابد من المحافظة على سريتها وسلامتها وحمايتها من أي اعتداء يطالها، **ومن خلال دراستنا لهذا الموضوع توصلنا إلى عدة نتائج أهمها:**

- قد تكون البيانات الشخصية للمستخدم بيانات عادية يتم الإدلاء بها عند إبرام عقد الحوسبة السحابية كاسمه ولقبه وتاريخ ميلاده ورقم هاتفه وعنوان بريده الإلكتروني، وقد تكون بيانات حساسة تقوم المؤسسات والأفراد بتخزينها على السحابة، وهي بيانات تكتسي طابعا شخصيا وتظهر الأصل العرقي الشخص أو آرائه السياسية أو معطياته الجينية...

- يلعب الأمان السحابي دورا مهما في الحفاظ على سرية وسلامة البيانات الشخصية في إطار عقود الحوسبة السحابية، وينقسم إلى أمن داخلي يهدف إلى حماية البيانات المخزنة، وأمن خارجي يهدف إلى حماية البيانات عند انتقالها من وإلى السحابة.

– تتعرض البيانات الشخصية المخزنة سحابيا إلى مخاطر كبيرة وهجمات سيبيرانية كالوصول غير المصرح به للبيانات أو الكشف عنها أو إساءة استعمالها أو قرصنتها أو فقدانها، وقد يقع الهجوم على السحابة داخليا من طرف الأشخاص العاملين على تقديم الخدمة السحابية، وقد يكون خارجيا من طرف قراصنة الإنترنت.

– عقد الحوسبة السحابية عقد ملزم لجانبين، ومن أهم الالتزامات الواقعة على عاتق مزود الخدمة توفير الحماية الكافية للبيانات الشخصية التي يتولى تخزينها وضمان أمنها وسلامتها، وفي حالة مخالفة ذلك تقوم مسؤوليته العقدية إذا توفرت أركانها، إضافة إلى قيام المسؤولية التقصيرية لمرتكب الاعتداء إذا كان الهجوم خارجيا.

– دعم المشرع الجزائري الحماية المدنية المقررة للبيانات الشخصية بالحماية الجزائية، وهو ما يظهر أساسا من خلال جريمة الدخول بطريقة غير مشروعة إلى النظام المعلوماتي للحوسبة السحابية أو البقاء غير المشروع فيه، ناهيك عن الجرائم المتعلقة بالمعالجة الآلية للبيانات الشخصية إذا كانت محلا لهذه المعالجة.

– نظرا لعدم كفاية الحماية القانونية للبيانات الشخصية في إطار الحوسبة السحابية، فكان لابد من استعمال الوسائل التقنية للحماية كالتشفير والجدران النارية وأنظمة الكشف على الاختراقات لتدعيم الحماية القانونية، لأنه لا يمكن الرد على الآلة إلا من خلال الآلة، لكن مهما أحرزت هذه الوسائل التقنية من تقدم فلا يمكنها أن تضمن بشكل مطلق حماية البيانات الشخصية ضد مخاطر الهجمات السيبيرانية.

انطلاقا مما تقدم يمكننا تقديم التوصيات التالية:

– يتعين على مقدمي الخدمات السحابية الالتزام الدائم والمستمر بالقوانين واللوائح المتعلقة بحماية البيانات الشخصية للمستخدم لا سيما الحساسة منها.

– يتعين على المستخدم أن يختار بعناية مقدم خدمات سحابية تتوفر فيه الموثوقية، ويتبنى أعلى مستويات الحماية للبيانات الشخصية التي يتولى تخزينها على خوادمه من أجل تفادي أي تهديدات سواء كانت داخلية أو خارجية.

– يتعين على مقدمي الخدمات السحابية اتباع أكثر التقنيات تطورا لحماية البيانات الشخصية، وأن يقوموا بالتحديث الدائم للبرامج والسياسات الأمنية بهدف سد مختلف الثغرات وتقليص فرص الهجمات الإلكترونية والاختراقات.

– مسؤولية حماية البيانات الشخصية هي مسؤولية مشتركة، لذا إضافة إلى تدابير الحماية التقنية التي يوفرها مزود الخدمة السحابية يتعين على المستخدم المحافظة على سرية معلومات الاتصال وعدم الإفصاح عنها للغير.

– ضرورة أن يقوم المشرع الجزائري باستحداث نصوص قانونية تنظم عقود الحوسبة السحابية وما يرتبط بها من مسائل قانونية على غرار حماية البيانات الشخصية.

– يتعين على المؤسسات التي تريد التوجه إلى اعتماد الحوسبة السحابية إجراء موازنة بين ما تقدمه هذه التكنولوجيا الحديثة من مزايا وما يترتب عنها من مخاطر، ومدى تأثير ذلك على أداء هذه المؤسسات.

الهوامش:

[1] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية: دراسة مقارنة، (ط1)، مركز الدراسات العربية، مصر، 2016، ص29.

[2] علي نعمة جواد الزرفي، الجريمة المعلوماتية الماسة بالحياة الخاصة: دراسة مقارنة، (د. ط)، المكتب الجامعي الحديث، الإسكندرية، 2020، ص95.

[3] القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المؤرخ في 10 يونيو 2018، ج.ر عدد 34، الصادرة في 10 يونيو 2018.

[4] V : LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[5] أما بعد تعديل القانون الفرنسي رقم 78-17 سنة 2018، بموجب القانون رقم 493-2018 المؤرخ في 20 جوان 2018 والمتعلق بحماية البيانات الشخصية تم تعديل المادة 2 المذكورة وأورد المشرع الفرنسي تعريفا لملف البيانات الشخصية.

V: JORF n°0141 du 21 juin 2018.

[6] سمير سعد رشان سلطان، الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات "دراسة مقارنة"، مجلة البحوث القانونية والاقتصادية، عدد 88، يونيو 2024، ص1043.

[7] Sarah Sadik, la protection des donnés dans les contrats de cloud computing, spécialité droit privé, thèse de doctorat, université de Perpignan, 2023, p33.

[8] قرار مجلس سلطة الضبط رقم 48/ أ خ/ر م/س ض ب م/ 2017، المؤرخ في 2017/11/29 المتضمن المصادقة على دفتر الشروط المحدد لشروط وكيفيات إقامة واستغلال خدمات استضافة وتخزين محتوى معلوماتي لفائدة مستعملين متباعدين في إطار الخدمات المعلوماتية المسماة الحوسبة السحابية.

[9] خالد ممدوح إبراهيم، التنظيم القانوني للبيانات الرقمية في الفضاء السيبراني (الحوسبة السحابية)، (ط1)، دار الفكر الجامعي، الإسكندرية، 2023، ص.ص38.39.

[10] محمود إسماعيل أبو ترابي، التنظيم القانوني لعقود الحوسبة السحابية في ظل القانون الأردني، المجلة الأردنية للعلوم التطبيقية، المجلد 17، العدد 1، 2015، ص97.

[11] خالد ممدوح إبراهيم، مرجع سابق، ص51.

[12] المرجع نفسه، ص21 وما بعدها.

[13] باسم محمد فاضل مدبولي، المسؤولية المدنية عن أضرار معالجة البيانات الرقمية: دراسة مقارنة، (ط1)، دار الفكر الجامعي، الاسكندرية، 2023، ص35.

[14] ج. ر عدد 28 مكرر (هـ)، صادرة في 15 يوليه 2020.

[15] محمود إسماعيل أبو ترابي، مرجع سابق، ص90.

[16] ناصر أبو زيد الكشكي، التخزين الآمن للبيانات على الحوسبة السحابية: دراسة تقييمية، مجلة التعليم عن بعد والتعليم المفتوح، المجلد 2، العدد 2، مايو 2014، ص99.

[17] خالد ممدوح إبراهيم، مرجع سابق، ص53.

[18] ناصر أبو زيد الكشكي، مرجع سابق، ص110.

[19] أنظر الموقع الإلكتروني: https://www.microsoft.com/ar/security/business/security-101/what-is-ransomware تاريخ الزيارة: 20 نوفمبر 2024، على الساعة 16:30.

[20] خالد ممدوح إبراهيم، مرجع سابق، ص167.

[21] نبيلة إسماعيل رسلان، المسئولية في مجال المعلوماتية والشبكات، (د. ط)، دار الجامعة الجديدة، الإسكندرية، 2007، ص33.

[22] محمود إسماعيل أبو ترابي، مرجع سابق، ص96.

[23] أنظر المادة 38 من القانون 18-07.

[24] أنظر المادة 7 من القانون 18-07.

[25] أنظر المادة 9 من القانون 18-07.

[26] أنظر المادة 32 من القانون 18-07.

[27] الأمر رقم 75- 58 المؤرخ في 26 سبتمبر 1975، يتضمن القانون المدني، ج. ر عدد 78، الصادرة في 30 سبتمبر 1975، المعدل والمتمم.

[28] باسم محمد فاضل مدبولي، مرجع سابق، ص200.

[29] معاذ محمود يوسف العمري، النظام القانوني للحق في البيانات الشخصية عبر الوسائل الإلكترونية، رسالة ماجستير، جامعة اليرموك، الأردن، 2015، ص73.

[30] أنظر المادة 40 من القانون 18-07.

[31] وقد سار في هذا الاتجاه: محمد صبري الجندي، في المسؤولية التقصيرية -المسؤولية عن الفعل الضار- دراسة في الفقه الغربي والفقه الإسلامي والقانون المدني الأردني، (ط1)، دار الثقافة، عمان، الأردن، 2015، ص70.

[32] الأمر رقم 66-156 المؤرخ في 8 يونيو 1966، يتضمن قانون العقوبات المعدل والمتمم، ج. ر عدد 49، الصادرة في 11 يونيو 1966.

[33] خالد ممدوح إبراهيم، مرجع سابق، ص176.

[34] غنية باطلي، الجريمة الإلكترونية: دراسة مقارنة، (د. ط)، الدار الجزائرية للنشر، الجزائر، 2015، ص160.

[35] خالد ممدوح إبراهيم، مرجع سابق، ص190.

[36] أنظر: المادة 2/394 مكرر من (ق. ع. ج).

[37] أنظر: المادتين 73 و74 من القانون 18-07.

[38] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي: النظام القانوني للحماية المعلوماتية، (د. ط)، دار الجامعة الجديدة، الإسكندرية، 2009، ص576.

[39] رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الإنترنت: دراسة مقارنة، (د. ط)، دار النهضة العربية، القاهرة، 2013، ص277.

[40] Ari Juels and Tomas Ristenpart, Honey Encryption : Security Beyond the Brute-Force Bound, Eurocrypt 2014, 33 rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014, Springer publishing, New york, p293.

[41] Sarah Sadik , Op.Cit, p50.