

Le cloud computing : quelles sont les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées?

Nassima BOURZAMA

LE CLOUD COMPUTING : QUELLES SONT LES MESURES PRISES, EN ALGÉRIE, POUR SÉCURISER LES DONNÉES PROFESSIONNELLES HÉBERGÉES?

CLOUD COMPUTING: MEASURES TAKEN, IN ALGERIA, TO SECURE HOSTING PROFESSIONAL DATA

Nassima BOURZAMA

Doctorante, Université d'Alger 3

Bourzama.nassima@gmail.com

Date de soumission 2018-04-20	Date d'acceptation 2018-12-04	Date de Publication 2018-12-15
----------------------------------	----------------------------------	-----------------------------------

Résumé:

La propagation de la technologie Cloud Computing, avec ses différents modèles de services (SaaS, PaaS, IaaS) et modes de déploiement, a poussé les États et les autorités de régulation à mettre en place les mécanismes nécessaires pour minimiser les risques de sécurité liés à l'utilisation de cette technologie.

Afin de sécuriser les données professionnelles hébergées dans le Cloud, l'Algérie a commencé à adapter la réglementation et à définir les outils permettant le développement de cette technologie dans le pays.

Mots clés : Cloud Computing ; SaaS/PaaS/IaaS ; Sécurité des données ; Cadre juridique ; Algérie.

Abstract: The propagation of Cloud Computing technology, with its different service models (SaaS, PaaS, IaaS) and deployment modes, has prompted States and regulators to implement the necessary mechanisms to minimize the security risks associated with the use of this technology.

In order to secure business data hosted in Cloud, Algeria has started to adapt the regulation and to define the tools allowing the development this technology in the country.

Keywords: Cloud computing;SaaS/PaaS/IaaS;data security;legal framework; Algeria.

1-Introduction :

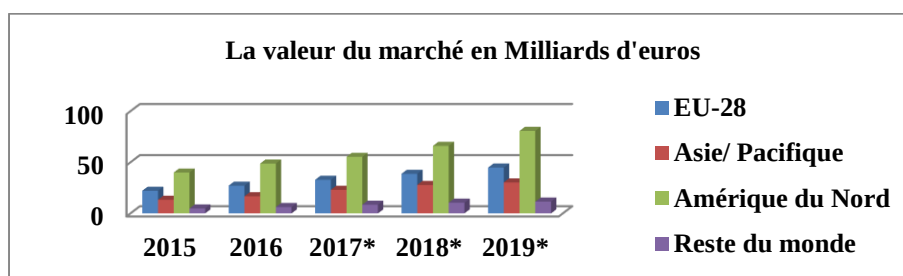
Avec le développement massif qu'a connu le réseau internet depuis son apparition au début des années 90 ; les entreprises ont commencé à adopter de nouvelles approches pour booster leurs systèmes d'information.

En conséquence, une évolution constante de ces systèmes au niveau des entreprises s'est traduite par le passage de l'infogérance classique à l'infonuagique, d'où le concept « Cloud Computing ».

Considérée comme l'une des principales innovations technologiques du 21^{ème} siècle, la technologie Cloud Computing s'est propagée rapidement dans différents secteurs (Banques, Assurances, Petites et Moyennes Entreprises, ...).

D'après des statistiques publiées par Statistica, le graphique ci-dessous indique la valeur du marché des services Cloud Computing pour les entreprises, par région du monde, en 2015 et 2016, et présente des prévisions pour les années 2017, 2018 et 2019.

La valeur du marché du Cloud Computing dans le monde a connu une augmentation de 23,22 % entre l'année 2015 et 2016. Selon le même site, cette valeur pourrait atteindre 167,3 Milliards d'euros en 2019, soit une hausse de 108,89% par rapport à 2015.



Source : <https://fr.statista.com> : <https://fr.statista.com/statistiques/555926/cloud-computing-ind-entreprises-valeur-marche-mondial-continent> , consulté le 12/12/2017 à

14h 23min

En effet, cette évolution notable du Cloud dans le monde a poussé les entreprises d'une part et les Etats d'autre part à veiller pour une meilleure prise en charge de tous les facteurs qui peuvent contribuer au bon développement de cette technologie, dont la sécurité des données hébergées constitue l'un de ses défis majeurs.

En Algérie, le Cloud Computing est apparu en 2013 par la société ISSAL, qui « héberge le premier Cloud du pays et de la région » (<http://issal.dz/a-propos/> Consulté le, 04/05/2016 à 23h:54min).

La taille du marché de Cloud Computing et son évolution en Algérie, comme dans les pays voisins, reste timide par rapport à la valeur et au volume importants des entreprises qui activent dans la sphère économique de cette région.

La problématique de sécurité des données hébergées dans le Cloud constitue un frein majeur pour la plupart des entreprises qui ont déjà migré vers cette solution et celles qui envisagent de l'adopter. De plus, avec l'apparition des lois qui cadrent l'utilisation du Cloud dans les pays du monde, les États sont devenus de plus en plus réticents vis-à-vis son utilisation.

Dans ce contexte, afin de faire face aux risques liés au Cloud, les États ont mis en place des mesures réglementaires pour protéger les données hébergées circulants au sein ou en dehors de leurs territoires.

De son côté, l'Algérie a commencé à adapter son cadre juridique pour prendre en charge les risques qui peuvent menacer la sécurité des données professionnelles hébergées dans le Cloud.

Cet article a pour objectifs d'une part, de comprendre la technologie du Cloud Computing (Caractéristiques, modèles de services et modes de déploiement), d'exposer les risques liés à son utilisation et d'autre part, d'étudier à quel niveau la sécurisation des données professionnelles stockées dans le Cloud est prise en charge en Algérie.

2-Comprendre le Cloud Computing :

2-1Définition :

Il est vrai qu'une définition exacte du concept « Cloud Computing » n'est pas encore apparue, mais dans cet article, nous allons nous baser sur un extrait de définition de NSIT¹ et d'un groupe spécialisé de l'UIT², qui définissent le Cloud Computing comme suit: «Le Cloud computing est un modèle qui offre aux utilisateurs du réseau un accès, à la demande, à un ensemble de ressources informatiques partagées et configurables, et qui peuvent être rapidement mises à la disposition du client sans interaction directe avec le prestataire de service.» (ITU, 2012).

D'après cette définition, le Cloud Computing n'est qu'une nouvelle façon de délivrer les ressources informatiques et se distingue de l'infogérance classique à travers plusieurs caractéristiques.

2-2Caractéristiques du Cloud Computing :

D'après (Romain Hennion et Al,2012), les cinq caractéristiques fondamentales du Cloud sont résumé escomme suit :

➤ **Service à la demande**

L'utilisateur du Cloud peut accéder immédiatement, à sa demande, à des services informatiques fournis par le prestataire de service.

➤ **Service mesuré (Pay As You Go)**

Les utilisateurs payent les ressources, qu'ils utilisent, en fonction de leur consommation réelle et précise (Plouin, Guillaume, 2016) ; toutefois, les Directeurs Systèmes d'Information trouvent, actuellement, des difficultés techniques pour mesurer, exactement, leur consommation informatique chez le fournisseur Cloud.

¹ NSIT : National Institute of Standards and Technology.

² UIT : Union Internationale des Télécommunications.

➤ Bande passante élevée

Grâce aux capacités des réseaux, les services Cloud sont accessibles depuis plusieurs plates-formes (PC, téléphones mobiles, ordinateurs portables, etc.).

➤ Partage des ressources

Les utilisateurs Cloud partagent les mêmes ressources, d'où une réduction des coûts d'utilisation (économie d'échelle).

➤ Élasticité

En cas d'évolution de ses besoins métier, l'utilisateur peut facilement acquérir de nouvelles ressources et/ou développer la puissance des ressources existantes.

Ces spécificités font de la technologie Cloud Computing une nouvelle option qui offre à ses utilisateurs la possibilité d'accès à des logiciels et à des ressources informatiques avec la flexibilité et la modularité souhaitées et à des coûts très compétitifs (ITU, 2012).

2-3 Modèles de services du Cloud Computing :

Il existe trois (03) principaux modèles de service du Cloud :

➤ Infrastructure as a Service (IaaS)

Il s'agit de location de plateforme technique, permettant l'exécution d'architectures applicatives complètes, comprenant base de données, serveur d'application, etc. (Plouin, Guillaume, 2016). Ce modèle permet à l'utilisateur de minimiser les coûts d'investissement relatifs à l'acquisition d'une telle infrastructure.

➤ Plateforme as a Service (PaaS)

Il s'agit d'un Cloud qui s'adresse principalement aux développeurs et aux producteurs d'applications.

Selon le (CIGREF³, 2013), le PaaS permet de fournir deux niveaux de service :

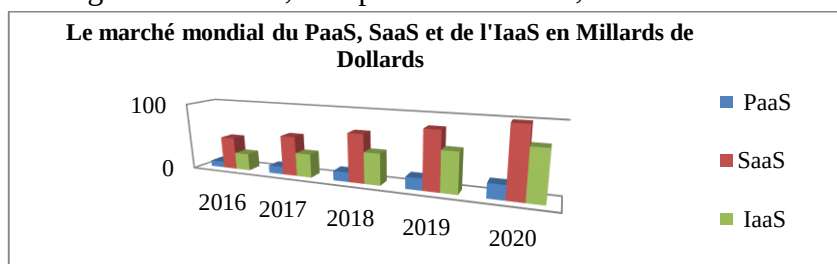
³CIGREF : Club Informatique des Grandes Entreprises Françaises.

- Mettre à disposition des développeurs un framework de développement adapté à leurs besoins.
- Donner aux applications un cadre d'exécution qui produira des services SaaS.

➤ **Software as a Service (SaaS)**

Il s'agit de la location d'une application opérationnelle et des services associés sans passer par l'étape de l'installation ; ce type de service s'adresse aux utilisateurs finaux.

Selon Gartner, le SaaS présente le modèle du Cloud le plus porteur dans le monde, ses revenus ont atteint 48,2 Milliards de dollars en 2016, soit cinq (05) fois supérieurs au chiffre d'affaires généré par le PaaS et deux (02) fois à celui de l'IaaS. Cette étude prévoit aussi que le SaaS va rester leader sur le marché mondial jusqu'à 2020, et son chiffre d'affaire pourrait augmenter de 106,85% pour atteindre 99,7 Milliards de Dollars.



Source : Réalisé à partir des données de la table 1. "Worldwide Public Cloud Services Revenue Forecast (Billions of U.S. Dollars)" / Gartner (Octobre, 2017), publiée sur: <https://www.informatiquenews.fr/marche-mondial-cloud-public-croissance-de-185-54078>, consulté le 10/12/2017, à 19h:33 min.

2-4 Modes de déploiement du Cloud Computing :

Le Cloud Computing peut être utilisé sous plusieurs modes de déploiement ; le choix du mode adéquat se fait en fonction de la vision et des objectifs fixés par l'entreprise.

➤ **Cloud privé**

Dans ce mode, l'entreprise possède ou loue un datacenter qui reste au sein de cette dernière. La gestion de l'infrastructure Cloud est confiée à l'entreprise elle-même dont le but est de répondre à ses propres besoins.

Cette solution permet de ne pas transférer des données sensibles sur un serveur externe, autorise le maintien d'avantages comparatifs liés à des applications développées en interne et dont il n'existe pas d'équivalent (Grégoire Tiers et al. 2013).

➤ Cloud public

Le fournisseur du service Cloud possède une infrastructure technique dont les services sont mis à la disposition des entreprises utilisatrices. Ce mode est généralement adopté par les institutions qui ne peuvent pas supporter les coûts d'acquisition des ressources informatiques.

➤ Cloud communautaire

L'infrastructure est partagée par plusieurs organisations et concerne une communauté spécifique qui partage des intérêts communs (une mission, des exigences de sécurité, des obligations légales, etc.) (Romain Hennion et Al., 2012).

➤ Cloud hybride

Il s'agit d'une combinaison simultanée entre les ressources du Cloud privé et celles du Cloud public. Il permet à l'entreprise de bénéficier des avantages du Cloud tout en gardant le contrôle sur ses données critiques.

➤ Cloud souverain

Le Cloud Computing peut être défini comme « un enjeu stratégique, qui relève de la souveraineté des États (Jean-Marc Sauvé, 2013) ». Dans ce contexte, un rapport sur le Cloud Computing en Belgique a présenté le Cloud souverain comme un « Cloud qui combine les clouds public et communautaire à l'échelle d'un pays afin, notamment, de se rattacher à un cadre juridique et économique déterminé » (l'UNISYS Corporation ,2013).

Ce mode de déploiement a été choisi par plusieurs pays dont la France ; une note d'information du Ministère de l'intérieur français (Ministère de l'intérieur, 2016) a défini le Cloud souverain comme un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de Cloud physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et des normes françaises.

Selon (Maya Dan, 2014), l'historique de ce type de Cloud remonte au Patriot Act⁴. La France, comme la Grande Bretagne ou l'Allemagne, ont décidé de bâtir un Cloud local. Ce Cloud souverain devait servir à stocker des informations sensibles telles que des données personnelles administratives, des renseignements liés à l'e-santé ou encore des informations économiques nécessitant un maximum de sécurité.

En Europe, le cadre juridique relatif à la protection des données est toujours en développement.

Un communiqué de la Commission Nationale d'Informatique et des Libertés (CNIL), en France, a indiqué que le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne et entrera en application le 25 mai 2018. L'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique (<https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>).

Consulté le 10/02/2017 à 22h:46min.).

2-5 Risques associés au Cloud Computing :

La culture, généralement, répandue dans le monde entreprise fait que le maintien des données informatiques au niveau local donne lieu, automatiquement, à une sécurité assurée. Pour ces entreprises, l'externalisation (Cloud Computing) est considérée comme un risque inévitable et logique. Selon (Plouin Guillaume, 2016) le principal frein à l'adoption du Cloud est la question de la sécurité des données, chez 64% de décideurs IT et 45% de décideurs métiers.

Cependant, nous rappelons que la confiance mise vis-à-vis de n'importe quel nouveau mode de gestion (qu'il soit technologique ou autres) ne pourra s'installer que dans le temps.

En effet, l'entreprise adoptant ou envisageant d'adopter le Cloud Computing doit prendre en considérations d'une part, les aspects relatifs

⁴L'acronyme Patriot (pour providing appropriate tools required to intercept and obstruct terrorism, soit « fournir les outils appropriés pour déceler et contrer le terrorisme »).

Le cloud computing : quelles sont les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées?

Nassima BOURZAMA

aux risques provenant de cette solution et d'autres part, les mesures nécessaires pour les minimiser.

Dans son rapport publié en 2010, l'ANSSI⁵ (France) a cerné les différents risques pouvant être associés à l'informatique dans les nuages. Ces derniers sont résumés comme suit:

2-6 Risques liés à la localisation des données :

Dans un Cloud public, les données peuvent être déplacées très rapidement d'un data center à un autre, donc d'un État à un autre et ce, en fonction des ressources disponibles chez le fournisseur de service.

En Europe, malgré l'existence d'un cadre juridique sur la protection des données à caractère personnel, la mise en place des services de Cloud Computing fait encourir l'entreprise à des risques liés à ces données. « Ces risques sont aggravés en cas de transfert de données hors de l'Union Européenne (UE) » (<http://www.murielle-cahen.com/publications/p-cloud.asp>, consulté le 14/03/2017, à 18h:45min.).

Le danger est dû à l'impossibilité de localiser les données dans le Cloud public, ce qui pose problème de la compétence des juridictions et du droit applicable.

Selon (ANSSI, 2010), une localisation de données non maîtrisée peut comporter d'autres risques qui sont liés, essentiellement, aux difficultés de :

- Exercer un droit de regard et de contrôle sur les personnels du prestataire;
- Effectuer un audit de sécurité de l'infrastructure sous-jacente ;
- Répondre à d'éventuelles injonctions de la justice.

La rédaction de contrats de Cloud Computing devra donc également prendre en considération ces problématiques (<http://www.murielle-cahen.com/publications/p-cloud.asp>, consulté le 07/04/2017, à 21h:16min.).

⁵ ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

2-7 Risques de perte de maîtrise du système d'information :

➤ Perte de gouvernance

En se lançant dans une solution Cloud Computing, la Direction de Système d'Information de l'entreprise perd le contrôle total sur ses activités. La maîtrise des tâches relatives à la sécurisation du système devient une mission de plus en plus lourde et étrange pour la DSI.

➤ Dépendance technologique

Avant la signature d'un contrat d'hébergement Cloud Computing, l'entreprise doit veiller à garantir la portabilité des données, des applications et des services et ce, malgré que la plupart des offres ne comportent pas cette possibilité.

➤ Risques liés à la mutualisation des ressources

Connu sous l'appellation « CIA : Confidentiality, Integrity and Availability », le triangle : Confidentialité, intégrité et disponibilité des données constitue la préoccupation majeure des décideurs lors d'une migration vers le Cloud.

D'après (CNIL,2012),il est indispensable de définir et de mettre en place les mesures nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données : par exemple, chiffrement des données et procédés garantissant ainsi que le prestataire n'a pas accès aux données qui lui sont confiées (chiffrement côté client, avec un algorithme reconnu et une gestion des clés adéquate, avant tout transfert) et liaison chiffrée avec le serveur de Cloud (connexion de type https ou VPN par exemple).

De son côté, le référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (Cloud Computing) publié par l'ANSSI (ANSSI, 2014) mentionne que la perte d'intégrité des informations est susceptible d'avoir des incidences importantes et globales au niveau de l'organisation. Une perte d'intégrité doit être immédiatement détectée et corrigée.

3-Le Cloud Computing : Les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées :

Consciente des opportunités offertes par les technologies de l'information et de communication, l'Algérie a pris les mesures nécessaires pour favoriser davantage le développement de ce domaine dans les différents secteurs (Administrations, enseignement, santé, économie,...).

3-1La réglementation du Cloud Computing en Algérie :

La mise à jour du cadre réglementaire régissant les technologies de l'information et de communication a toujours été une action primordiale qui accompagne le développement technologique en Algérie. Cette action permet d'une part de favoriser la mise en place des nouvelles technologies dans le pays et d'autre part, de sécuriser l'environnement dans lequel ces technologies s'exercent et se propagent.

L'ancrage juridique du secteur des TIC est passé d'abord par une étape de monopole, étape durant laquelle l'Etat algérien était le fournisseur direct et unique des activités des télécommunications.

Ensuite, et afin de s'adapter au contexte mondial de l'environnement technologique, une réforme juridique du secteur des TIC a permis son ouverture à la concurrence. Il s'agit de la loi 2000-03 fixant les règles générales relatives à la poste et aux télécommunications « qui a introduit les mécanismes de marché dans le secteur de la poste et des TIC» (<http://www.mpttn.gov.dz/fr/content/réglementation>. Consulté le, 20/08/2017 à 00h:03min).

Cette loi a donné lieu à la création de l'Autorité de Régulation de la Poste et des Télécommunications (ARPT) dont la mission principale, telle que définie par la loi, est de veiller à la mise en place des conditions favorables pour l'émergence et le développement d'une concurrence viable sur le marché des télécommunications.

La technologie Cloud computing, en Algérie, est l'une des activités qui appartiennent au secteur de télécommunications. De ce fait, sa gestion relève des prérogatives et des attributions du Ministère de la Poste, des Télécommunications, des Technologies et du Numérique

(MPTTN) et précisément, de l'Autorité de Régulation de la Poste et des Télécommunication.

La réglementation des fournisseurs de Cloud, en Algérie, est passée par deux phases :

1. Avant la publication de la décision N° 48/SP/PC/ARPT/17 :

Avant la publication de ladite décision, les fournisseurs Cloud activaient dans le cadre de l'autorisation des Fournisseurs d'Accès Internet (FAI) délivrée par l'ARPT. Ces derniers ont été soumis aux dispositions de l'article 3 du décret exécutif n° 15-320 du 13 décembre 2015 fixant le régime d'exploitation applicable à chaque type de réseaux, y compris radioélectriques et aux différents services de télécommunications, qui prévoit la fourniture des services rentrant dans le cadre de l'hébergement, les Datacenter et le Cloud computing. Selon cet article (JORADP, 2015) :« Sont subordonnés à l'octroi d'une autorisation délivrée par l'autorité de régulation de la poste et des télécommunications, l'établissement et l'exploitation de (...) :

- Services d'hébergement et de stockage de contenu informatisé au profit d'utilisateurs distants dans le cadre des services dits d'informatique en nuage ou Cloud Computing (...) ».

2. Après l'approbation et la publication de la décision N° 48/SP/PC/ARPT/17 du 29/11/2017 portant approbation du cahier des charges définissant les conditions et les modalités d'établissement et d'exploitation des services d'hébergement et de stockage de contenu informatisé au profit d'utilisateurs distants dans le cadre des services dits informatique en nuage ou Cloud Computing.

Cette décision qui a défini le Cloud Computing, en Algérie, comme « un modèle permettant d'offrir un accès via le réseau à un ensemble modulable et élastique de ressources physiques ou virtuelles mutualisables, approvisionnées et administrées à la demande et en libre-service » a soumis les fournisseurs de Cloud en Algérie aux dispositions législatives réglementaires nationales et internationales. Il s'agit principalement de :

Le cloud computing : quelles sont les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées?

Nassima BOURZAMA

- La loi n° 2000-03, modifiée et complétée, fixant les règles générales relatives à la poste et aux télécommunications.
- La loi n° 09-04 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.
- Le décret exécutif n° 15-320 correspondant au 13 décembre 2015 relatif au régime d'exploitation applicable à chaque type de réseau, y compris radioélectrique et aux différents services de télécommunications.
- Règlements de l'Union Internationale des Télécommunications (UIT).

Le cahier des charges limite l'offre des services d'hébergement et de stockage de données octroyée par le fournisseur de Cloud en Algérie à trois (03) modèles de service, à savoir : IaaS, PaaS et SaaS. Ces derniers peuvent être offerts selon les modes de déploiement prévus par les recommandations de l'UIT/ISO en vigueur, à savoir : Cloud privé, Cloud public, Cloud hybride.

Pour obtenir l'autorisation, les fournisseurs de Cloud Computing doivent remplir deux conditions :

- 1- Introduire une demande auprès de l'ARPT.
- 2- Se constituer en la forme d'une société de droit algérien avec un siège social en Algérie.

Dans l'exercice de son activité, le fournisseur Cloud Computing est soumis aux obligations suivantes:

- « Offrir les services, selon les capacités disponibles, à tous les demandeurs en mettant en œuvre les moyens techniques les plus fiables ;
- Implanter son infrastructure sur le territoire national et garantir que celle-ci soit établie au moyen d'équipements intégrant les technologies les plus récentes et les plus avérées ;
- Garantir que les données des clients soient hébergées et stockées sur le territoire national ;

- Fournir les services via les infrastructures déclarées spécifiquement pour cette autorisation ;
- Assurer l'intégrité et la confidentialité des données des clients sauf dans les cas prévus par les textes en vigueur ;
- Assurer la disponibilité et la continuité du service fourni à ses clients sauf cas de force majeure ;
- Garantir une solution de sauvegarde " Backup " des données hébergées ou stockées ;
- Constituer un fichier d'identification des clients ;
- Ne pas divulguer ou utiliser les données des clients ;
- En cas de cessation de l'activité, de retrait ou de non-renouvellement de l'autorisation, le Titulaire est tenu de restituer les données des clients puis procéder à leurs suppressions physiques»(http://www.arpt.dz/Fr/doc/reg/dec/2017/DEC_N48_29_11_2017.pdf Consulté le 02/02/2018, à 23h:15min.).

3-2Le Référentiel National de Sécurité Informatique :

Dans le cadre de la mise en place des bonnes pratiques et des normes relatives à la sécurisation des données numériques en Algérie, un Référentiel National de Sécurité Informatique a été élaboré, en juin 2016, par le Ministère en charge de la Poste et des Technologies de l'Information et de Communication (Actuellement MPTTN).

Le Référentiel vise d'une part, à favoriser une meilleure protection des systèmes d'information au sein des organismes utilisateurs et d'autre part, à sensibiliser les usagers de la toile aux risques encourus et leur expliquer les bonnes pratiques en matière de prévention et de sécurité informatique (MPTIC,2016).

Dans le chapitre quatre relatif à la sécurité des systèmes, dont l'un de ses objectifs visés est d'assurer une sauvegarde des données dans le but de les récupérer en cas de perte, le Référentiel a interdit aux entreprises la sauvegarde des données professionnelles sur des sites de stockage

Le cloud computing : quelles sont les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées?

Nassima BOURZAMA

«Cloud» hébergeant les données en dehors du territoire national (MPTIC,2016).

Ce référentiel ne prend en charge que l'aspect relatif à la localisation des données stockées dans le Cloud ; d'autres aspects relatifs à la législation appliquée à l'internationale, aux conditions techniques de sécurité, à la qualification des fournisseurs Cloud et autres n'ont pas été abordés.

4-Conclusion:

Il est vrai que l'évolution des technologies, en Algérie, est prise en charge par la mise en place des textes juridiques adéquats, mais la lenteur des procédures d'élaboration, d'adoption et de publication de ces textes ne permet pas à ces derniers d'être à jour pour pouvoir suivre et accompagner, en temps réel, le rythme rapide du développement technologique que connaît le pays.

Dans ce contexte, l'activité d'offre des services Cloud Computing, qui était soumise (jusqu'à Novembre 2017) aux mêmes dispositions relatives aux Fournisseurs d'Accès Internet, est devenue actuellement réglementée à travers un cahier des charges dédié aux fournisseurs de Cloud Computing.

Les dispositions, citées dans cet article, ont pour principal objectif la protection des clients (personnes physiques ou morales) contre les différentes failles de sécurité pouvant menacer les données hébergées dans le Cloud Computing.

En outre, l'Algérie veille à renforcer la sécurisation des données hébergées à travers l'adoption, fin 2017, du projet de loi relatif à protection des personnes physiques dans le traitement des données personnelles.

Pour une meilleure prise en charge du développement de la technologie Cloud Computing en Algérie, des recommandations peuvent être formulées, il s'agit essentiellement de:

- Définir, clairement, les mécanismes de sécurité de l'information qui doivent être mis en place par les fournisseurs Cloud exerçant en Algérie et ce, conformément aux standards internationaux en matière de stockage, de traitement, de transfert et de sécurité des données hébergées dans le Cloud.
- Disposer d'un dispositif de contrôle et d'audit visant à superviser, sur le terrain, l'activité des prestataires Cloud Computing exerçant en Algérie.
- Former le personnel, les services juridiques et techniques au niveau des administrations, des banques, des sociétés d'assurances, des entreprises publiques et privées afin de favoriser le développement de cette technologie dans le pays.
- Opter pour la mise en place d'un Cloud souverain afin de réduire les coûts (infrastructure informatique, bande passante, etc.) et de garantir la souveraineté des données (à l'instar de l'expérience française).

Bibliographie:

- ANSSI, « *Maitriser les risques de l'infogérance* », Décembre 2010.P.8. Disponible sur : <<http://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques>>.
- ANSSI, « *Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (Cloud computing)* »- référentiel d'exigences Version 1.3 du 30/07/2014, P.12. Disponible sur : <https://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf>
- CIGREF, « *Fondamentaux du Cloud Computing*», Mars, 2013. P.8. Disponible sur : < <http://images.cigref.fr/Publication/2012-2013-Fondamentaux-Cloud-Computing-Point-de-vue-grandes-entreprises.pdf>>.
- Commission Nationale de l'Informatique et des Libertés (CNIL), « *Recommandations pour les entreprises qui envisagent de recourir à des services de Cloud computing* », 2012. Disponible sur :< https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf>.

Le cloud computing : quelles sont les mesures prises, en Algérie, pour sécuriser les données professionnelles hébergées?

Nassima BOURZAMA

- Grégoire Tiers et al. , « *L'envol vers le Cloud : un phénomène de maturations multiples* », Systèmes d'information & management 2013/4 (Volume 18), P. 7-42. DOI 10.3917/sim.134.0007.P.11.
- Jean-Marc Sauvé vice-président du Conseil d'État français, « *Le Cloud Computing* », Colloque de la société de législation comparée au Conseil d'État, 11/10/2013.P.10 .Disponible sur : < <http://www.conseil-etat.fr/Actualites/Discours-Interventions/Le-cloud-computing> >.
- Journal Officiel de la République Algérienne Démocratique et Populaire (JORADP), N° 68, du 27 décembre 2015. Correspondant au 15 Rabie El Aouel 1437. Article 3. P.10-11. Disponible sur : < <https://www.arpt.dz/fr/doc/reg/de/2015/DE15-320.pdf> >.
- Maya Dan, « *Bref historique des Cloud souverains* », La lettre du Cloud, édition spéciale sur le Cloud Souverain, N° 183 -18 Novembre 2014, P.5-6. Disponible sur : <<http://www.eurocloud.fr/doc/lettre-du-cloud-specialesouverain.pdf>>.
- Ministère de l'intérieur, « *Note d'information du 5 avril 2016 relative à l'informatique en nuage (Cloud computing)* », P.3. Disponible sur : <https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf>.
- Ministère de la Poste et des Technologies de l'Informations et de Communication (MPTIC), « *Référentiel de Sécurité Informatique* », Juin 2016.
- Plouin, Guillaume, « *Cloud computing : Sécurité, gouvernance du SI, hybride et panorama du marché* », Éd. 4, Éd. Dunod, 2016, P. 26, 21
- Romain HENNION, Hubert TOURNIER, Eric BOURGEOIS, « *Cloud computing : Décider-Concevoir-Piloter-Améliorer* ». Ed.1, Éd. EYROLLES, 2012. P.22.
- UIT, « *Le Cloud Computing en Afrique : Situation et Perspectives* », Avril 2012, P.3. Disponible sur : < https://www.itu.int/ITU-D/treg/publications/Cloud_Computing_Afrique-fr>.
- UNISYS Corporation (Patrice Emmanuel Schmitz et autres), Rapport sur : « *Le Cloud Computing. Une opportunité pour l'économie en Belgique* », 2013. P.8.Disponible sur: <http://economie.fgov.be/de/binaries/20130730_Cloud_computing_FR_tcm328-228881.pdf>.
- <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels>. Consulté le 10/02/2017 à 22h:46min.

- <http://www.murielle-cahen.com/publications/p-cloud.asp>, consulté le 14/03/2017, à 18h:45min.
- <https://fr.statista.com/statistiques/555926/cloud-computind-entreprises-valeur-marche-mondial-continent>, consulté le 12/12/2017 à 14 h 23min.
- <http://issal.dz/a-propos/> Consulté le, 04/05/2016 à 23 :54min.
- <https://www.informatiquenews.fr/marche-mondial-cloud-public-croissance-de-185-54078>, consulté le 10/12/2017, à 19h:33 min.
- <http://www.murielle-cahen.com/publications/p-cloud.asp>, consulté le 07/04/2017, à 21 :16min.
- <https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnelles>. Consulté le : 25/05/2016, à : 23h32min.
- <http://www.mpttn.gov.dz/fr/content/réglementation>. Consulté le, 20/08/2017 à 00h:03min.
- https://www.arpt.dz/fr/doc/reg/dec/2016/DEC_N51_03_04_2016.pdf.
- https://www.arpt.dz/fr/doc/reg/dec/2017/DEC_N10_22_02_2017.pdf Consultés le 01/05/2017, à 10h:23min.
- http://www.arpt.dz/Fr/doc/reg/dec/2017/DEC_N48_29_11_2017.pdf. Consulté le 02/02/2018, à 23h:15min.