Le Cloud computing ou la donnée dans les nuages

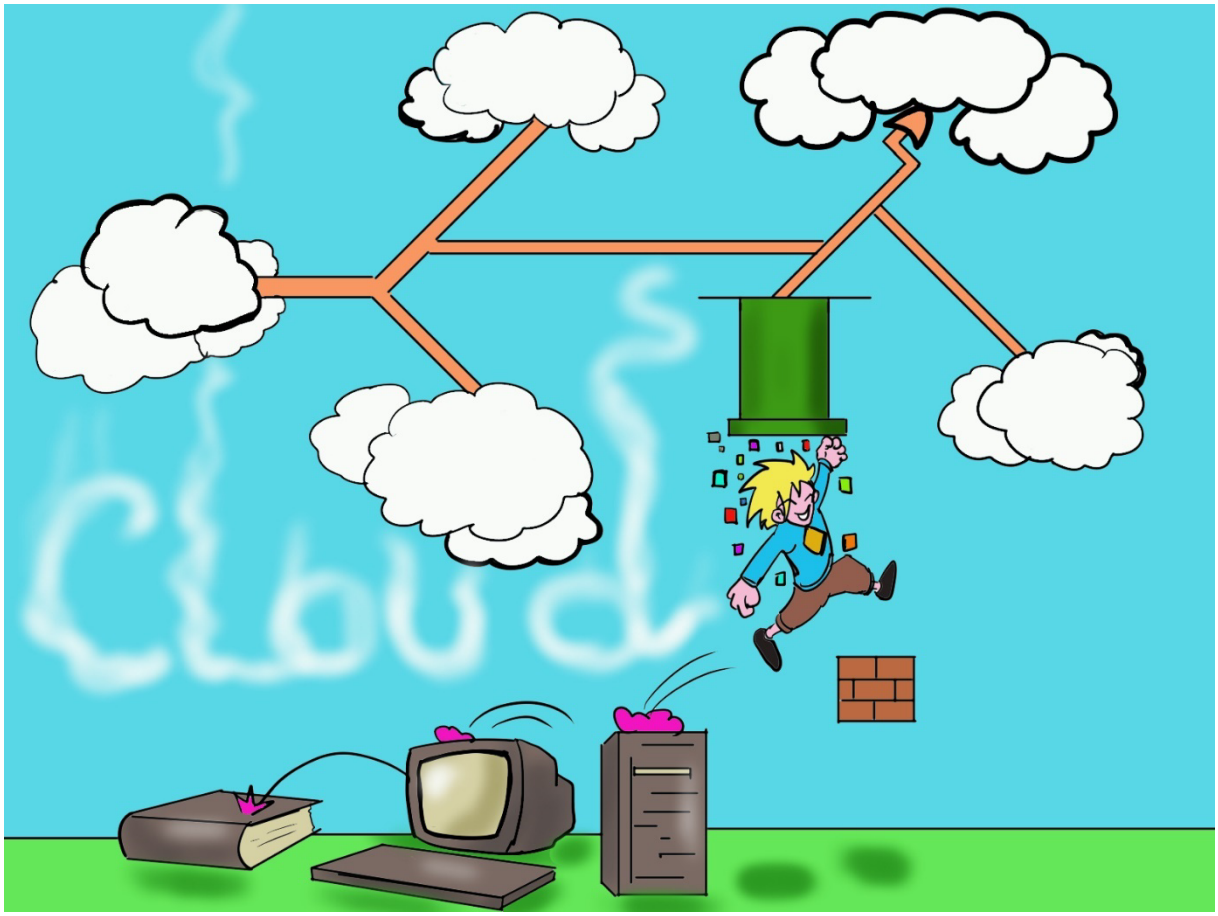
Traduit en français comme « *Informatique dans les nuages* », le Cloud computing ou Cloud est un système de stockage et d'outils qui s'est développé avec la numérisation de la société et qui ne cesse de croître.

Il permet aussi bien de stocker des données personnelles que d'utiliser des logiciels ou même encore de jouer.

En effet, au départ réservé aux professionnels, ce réseau extérieur est désormais utilisé par tout le monde, parfois sans même le savoir !

Ainsi lorsqu'une personne regarde une vidéo, sur Netflix par exemple, le film n'est en général pas téléchargé sur sa tablette, sauf si elle en fait la demande. Elle y accède donc par le cloud du diffuseur. Il en est de même lorsqu'il y a consultation des e-mails sur smartphone.

La condition d'accès au Cloud est ainsi d'avoir une connexion internet et un logiciel/une application qui permet l'enregistrement et la consultation des données.



Afin de vous permettre de mieux appréhender ce concept, cette fiche pratique a vocation à présenter le Cloud avec ses principaux avantages et inconvénients, et de mettre en exergue les questions principales qu'il peut poser en matière de protection des données.

Qu’est-ce que le Cloud computing ?

Si les termes de Cloud computing ou de Cloud ne font encore aujourd’hui l’objet d’aucune définition uniformisée, ils recouvrent **l'ensemble des solutions de stockage distant.**

En clair, les données, ou les outils, d’un utilisateur ou d’une entreprise (« *le client* ») ne sont plus sauvegardés sur son disque dur mais sont disponibles sur des serveurs distants accessibles par internet.

Ces données sont stockées par des infrastructures informatiques loin physiquement de celles du client dans d'immenses salles appelées **«** *Datacenter* » (centre de données). Ces salles, remplies de serveurs et d’ordinateurs très puissants qui offrent des outils et/ou **enregistrent, stockent, sauvegardent, protègent et administrent** toutes les données envoyées par tous.

Pour le commun des mortels, le Cloud n’est ainsi pas physique mais **virtuel**, et correspond à **un réseau de serveurs distants les uns des autres**, éparpillés sur la planète, mais reliés entre eux et fonctionnant comme un système seul ou bien maillé.

Il tire son nom du mot anglais signifiant « *nuage* » car au début des années 1990, il était courant de représenter Internet sous forme de nuage dans les schémas de réseaux.

Quant aux données enregistrées dans le Cloud, elles sont, dès connexion à celui-ci, accessibles **n’importe quand, n’importe où et de n’importe quel équipement** connecté à Internet.

Enfin, Il est important de noter que certains des systèmes qui utilisent le Cloud comme Google Drive ou iCloud, ont une base gratuite alors que d’autres ne le sont pas (Netflix ou Disney+ par exemple).

Quels sont les différents types de Cloud ?

Il existe quatre principaux types de Cloud.

Le Cloud public	Il s’agit d’un modèle de déploiement de Cloud où les ressources informatiques **n’appartiennent pas à l’utilisateur final** mais appartiennent à un fournisseur de service Cloud, à savoir une entreprise qui propose des infrastructures, des plateformes et/ou des logiciels via un réseau. Celui-ci exploite ces ressources informatiques et les partage à l’intention de plusieurs organisations et/ou individus. Lesdites ressources, accessibles par Internet, sont ainsi **ouvertes à tous et mutualisées**. Les données et applications de chaque client, à savoir toute personne s’exécutant dans le Cloud, restent toutefois isolées et cachées aux autres clients du Cloud.

	Le fournisseur est responsable de la maintenance des ressources et garantit la disponibilité, la fiabilité et la sécurité par le biais d'**accords de niveau de service**. C'est le modèle le plus répandu. **Exemples :** AWS (Amazon Web Services), Microsoft Azure
Le Cloud privé	Il s'agit d'un modèle dans lequel l'ensemble des ressources sont réservées via Internet ou sur un réseau interne à **l'usage exclusif d'un groupe d'utilisateurs ou d'une entité clairement défini(e).** Les ressources sont donc inaccessibles à toute personne extérieure. Les services d'un Cloud privé sont habituellement spécialement conçus pour répondre aux **besoins des clients que ce soit en termes de performance, de capacité de stockage et de réseau**. Ces derniers ont le choix entre héberger directement l'infrastructure du Cloud privé sur leur propre site (« *on-premise* ») ou bien potentiellement dans le centre de données du fournisseur. **Exemple :** OVH
Le Cloud hybride	Un Cloud hybride combine plusieurs types d'environnements Cloud, notamment les Clouds publics et privés, et peut également inclure des infrastructures hébergées sur site. Pour qu'un **Cloud soit réellement hybride**, il doit y avoir une **combinaison d'au moins 2 environnements** de Clouds qui échangent des informations entre eux et exécutent une série uniforme d'applications pour le compte d'un client. **Exemples :** - une combinaison d'au moins un Cloud privé et un Cloud public ; - une combinaison d'au moins deux Clouds publics ; - une combinaison d'au moins deux Clouds privés.
Le multi Cloud	Dans ce modèle, les clients exécutent des applications à l'aide de services Cloud provenant d'au moins deux fournisseurs de services Cloud afin de créer, exploiter, accéder et sécuriser lesdites applications de manière cohérente sur l'ensemble des Clouds. Cela permet également de minimiser la dépendance vis-à-vis d'un fournisseur. **Exemple :** Anthos, la plateforme hybride de Google Cloud

Quels sont les modes d'exploitation du Cloud ?

Le Cloud permet de rendre un certain nombre de **services** (outils bureautiques, messagerie, comptabilité, etc.) qu'il est possible de définir en fonction des **rôles** et des **usages** à la fois **des entreprises** qui fournissent le service et de celles qui utilisent ledit service.

Traditionnellement, 3 grands modes existent :

Le mode IaaS (Infrastructure as a Service)

Le Cloud permet de mettre en œuvre une **infrastructure virtuelle** (serveur, couches de virtualisation, stockage, réseaux) sur laquelle l'entreprise utilisatrice va pouvoir héberger des systèmes d'exploitation, des serveurs et des logiciels applicatifs.

Le fournisseur Cloud gère ainsi l'**infrastructure informatique uniquement** alors que de son côté le client gère lui-même l'installation, la configuration, les mises à jour du système d'exploitation, des « *middlewares* » (logiciels intermédiaires) et des applications, les données, etc.

Seule l'infrastructure matérielle est donc dématérialisée.

Gérés par le fournisseur	Virtualisation Serveurs Stockage Réseau
Gérés par le client	Données Applications Environnement d'exécution Conteneurs Système d'exploitation

Le mode PasS (Platform as a Service)

Le Cloud permet de mettre en œuvre une **plateforme d'exécution de logiciels et d'applications**, sur laquelle l'entreprise utilisatrice va pouvoir installer, configurer et utiliser les applications voulues

Avec cette solution, le fournisseur propose l'**infrastructure technique** mais également un **ensemble d'outils intégrés** qui permettent de développer des applications (système d'exploitation, base de données, etc.) et un serveur web. Le client lui se focalise sur le développement des applications.

Gérés par le fournisseur	Virtualisation Serveurs Stockage Réseau Environnement d'exécution Conteneurs Système d'exploitation
Gérées par le client	Données Applications

Le mode SaaS (Software as a Service)

Le Cloud fournit le **logiciel ou l'application**, regroupant les services de l'IaaS et du PaaS avec en plus, **l'installation, la maintenance et la configuration** comprises.

C'est une interface qui permet la **simple utilisation du logiciel** et ne nécessite pas de connaissance informatique ou technique au préalable.

Gérés par le fournisseur	Données Applications Environnement d'exécution Conteneurs Système d'exploitation Virtualisation Serveurs Stockage Réseau

En résumé :

Les modes d'exploitation	**IaaS**	**PaaS**	**SaaS**
Gérés par le fournisseur	Virtualisation Serveurs Stockage Réseau	Virtualisation Serveurs Stockage Réseau Environnement d'exécution Conteneurs Système d'exploitation	Données Applications Environnement d'exécution Conteneurs Système d'exploitation Virtualisation Serveurs Stockage Réseau
Gérés par le client	Données Applications Environnement d'exécution Conteneurs Système d'exploitation	Données Applications	

Quels sont les types de stockage Cloud ?

Ceux-ci sont au nombre de trois :

- **le stockage d'objets** : les objets stockent des données non structurées telles que des photos, des vidéos, des données issues du machine learning (ML), des données de capteurs, ou encore des fichiers audio.
  Ces données sont stockées par les objets dans le format dans lequel elles arrivent permettant ainsi de personnaliser les métadonnées de manière à faciliter l'accès aux données et leur analyse.
  Au lieu d'être organisés dans des fichiers ou des dossiers hiérarchisés, les objets sont conservés dans des compartiments sécurisés qui offrent une capacité de mise à l'échelle pratiquement illimitée.

- **le stockage de fichiers :** les applications utilisent très souvent un stockage basé sur les fichiers ou stockage sur fichier ce qui leur permet de stocker les données dans un dossier hiérarchique et un format de fichier.

- **le stockage de bloc :** ce stockage est utile pour les applications d'entreprise telles que les bases de données ou les systèmes de planification des ressources d'entreprise (ERP) qui nécessitent souvent un stockage dédié et à faible latence pour chaque hôte.
  Chaque bloc possède son propre identifiant unique pour un stockage et une récupération rapides.

Quels sont les avantages du Cloud ?

Les avantages du Cloud, pour les entreprises comme pour les particuliers, sont nombreux. Parmi ceux-ci figurent :

- **une réduction des coûts :** les structures n'ont plus besoin d'acquérir l'ensemble du matériel informatique autrefois indispensable pour leurs activités conduisant ainsi à une réduction des charges d'investissement de départ. Elles n'ont plus à obtenir des espaces de stockage ou du capital en plus lors des pics d'activité.
  Par ailleurs, l'absence, dans certains modèles, de maintenance et d'équipe technique dédiée permet de faire des économies. De même, le système d'abonnement offre aux clients la possibilité de ne payer que ce qu'ils consomment.

- **la flexibilité et l'évolution des services :** en fonction des besoins, il est possible d'augmenter ou de réduire l'utilisation des ressources informatiques proposées. En outre, les services gérés dans le Cloud sont mis à jour régulièrement.

- la possibilité d'un **stockage quasiment illimité :** les fournisseurs **construisent** en effet sans cesse de nouveaux centres de données.

- **un gain de temps :** le fournisseur Cloud gère lui-même un certain nombre de contraintes, telles que la maintenance, sans que le client n'ait à intervenir.

- l'accès à des services **de très haute qualité** sans payer des coûts prohibitifs.

- un **partage des données facilité** : tout utilisateur du Cloud peut rendre disponible ses données à un ou plusieurs autre(s) utilisateur(s) de ce cloud.

- une **accessibilité totale** : les applications sont conçues pour être accessibles partout, depuis n'importe quel appareil connecté ;

- **la sécurisation des données :** le Cloud offre un niveau de sécurité supérieur à un système classique composé de machines physiques. En effet, dès lors que les données sont dans le Cloud un ordinateur portable perdu ou volé n'est plus un soucis majeur.
  De plus, le stockage dans le Cloud permet de contrôler en permanence où sont stockées les données, qui peut y avoir accès et les ressources que le client consomme.

- **la continuité de l'activité :** les centres de données sont hautement sécurisés, protégeant ainsi les données et garantissant la continuité des activités. En cas de sinistre impactant les locaux du client (incendie par exemple), les données ne sont plus perdues.

Quels sont les inconvénients du Cloud ?

Malgré ses nombreux avantages, le Cloud Computing présente également des inconvénients, dont notamment :

- **la dépendance à internet :** en cas de panne, l'activité entière de la structure s'en trouve perturbée.

- **la dépendance technique par rapport aux fournisseurs Cloud:** la structure peut devenir tributaire du service proposé par un fournisseur. De plus, l'absence d'interopérabilité des systèmes peut l'empêcher de quitter son fournisseur.

- une **perte de contrôle** du système informatique : celui-ci n'est en effet plus sous le parfait contrôle de la structure et les applications utilisées peuvent changer à tout moment, au profit d'autres plus performantes ou plus adaptées au matériel du prestataire.

Quels sont les risques particuliers en matière de protection des données personnelles ?

Outre le nécessaire équilibre à trouver entre les avantages et les inconvénients du Cloud d'un point de vue pratique, il convient également de prendre en compte les risques que pose ce système de stockage en matière de protection des données personnelles.

Les données se trouvent en effet au cœur même des services offerts par le Cloud computing et comme dans tous projets informatiques, leur sécurité s'analyse en termes de **disponibilité, d'intégrité et de confidentialité** des données.

Les principaux risques sont ainsi les suivants :

- **un risque en matière de sécurité :** même si le niveau de sécurité proposé par les fournisseurs de service Cloud est élevé, les risques de pannes techniques et d'attaques informatiques ne peuvent être exclus, et ce d'autant plus que la concentration de toutes les données à un même endroit est particulièrement tentante pour les hackers. Le fait que les données transitent par Internet accroît également les risques.
- **un risque de perte de données** dans le cadre de procédures de sauvegardes ou de stockage.
- **un risque de fuite des données et de perte de confidentialité,** en raison du nombre de serveurs existants et de la délocalisation de ces derniers.
- **un risque de perte de contrôle** (ou de souveraineté sur les données), notamment quant à la localisation des données et à leur assujettissement aux lois et réglementations en vigueur sur le territoire national où figurent les serveurs (exemple : des données placées dans un Cloud, avec des serveurs basés aux États-Unis). De plus, de nombreux pays ont mis en place des législations ou des pratiques, comme le *Cloud Act* américain, qui leur permettent d'accéder aux données hébergées sur les services Cloud.

Le Cloud Act, qu'est-ce que c'est ?
Le Cloud Act (Clarifyng Lawful Overseas Use of Data Act) est une loi américaine qui permet aux Autorités judiciaires d'accéder aux données électroniques stockées à l'étranger par les entreprises américaines, dans le cadre de procédures pénales. En vertu de cette loi, il est donc possible pour le gouvernement US d'accéder aux serveurs en Europe et donc à Monaco à partir du moment où la société est américaine ou si la société a une relation d'affaires avec les Etats-Unis. Une étude publiée en août 2022 par le Ministère de la justice des Pays-Bas a conclu que les entités européennes peuvent être soumises à cette loi extraterritoriale même si leur siège social n'est pas aux Etats-Unis dès lors qu'elles utilisent des technologies américaines Elle précise même que le Cloud Act s'applique aussi quand un fournisseur de Cloud européen utilise du « *hardware* » ou un logiciel américain.

- un risque en matière de **transfert de données vers un pays ne disposant pas d'un niveau de protection adéquat**, subordonné par la Loi à certaines règles telles par exemples la mise en place de garanties appropriées (exemples : signature et mise en œuvre par les entités exportatrices et importatrices de données des clauses contractuelles types de la Commission européenne) ou encore dans de rares cas, l'autorisation préalable de l'APDP.

[Pour plus d'informations, voir la fiche pratique **Les transferts de données hors Principauté : les scénarios à envisager]**

Quelles mesures prendre pour sécuriser le Cloud ?

Si le risque zéro n'existe pas, plusieurs mesures permettent toutefois de protéger les données dans le Cloud, en tenant compte de facteurs tels que le type et la sensibilité des données à protéger.

Les principales mesures sont les suivantes :

La configuration du Cloud

Un grand nombre d'atteintes à la protection des données dans le Cloud sont dues à des vulnérabilités de base, comme des erreurs de configuration.

Afin de réduire ces erreurs, il est important :

- de modifier **les paramètres établis par défaut dans leur état d'origine** ;
- de ne **jamais laisser un « *bucket* »** (conteneur) **de stockage** dans le Cloud **ouvert** ;
- d'utiliser les **commandes de sécurité** proposées par le fournisseur de services

La sécurisation des comptes

Pour éviter que des logiciels malveillants ne s'introduisent dans les systèmes d'exploitation, des **logiciels antivirus et antimalware** doivent impérativement être installés et régulièrement mis à jour.

De même, **tous les appareils utilisés** pour accéder aux données dans le Cloud doivent être **sécurisés**, y compris les smartphones et tablettes. En effet, si les données sont synchronisées sur plusieurs appareils, les risques que l'un d'entre eux soit compromis et affecte les autres, augmentent.

La configuration des accès aux données

Toutes les personnes au sein d'une même structure ne sont pas nécessairement habilitées à avoir accès à toutes les informations disponibles dans le Cloud. Il est donc important que les équipes IT veillent à ce que les privilèges d'administrateur ne soient accessibles qu'à ceux qui en ont réellement besoin et que les comptes desdits administrateurs soient correctement sécurisés.

De même, il convient de s'assurer que l'accès aux données soit **limité aux seuls utilisateurs dûment habilités** et que ces permissions d'accès soient supprimées ou modifiées dès lors que les utilisateurs ne sont plus habilités à accéder à une ressource car ils ont quitté la structure ou changé de fonctions.

La sécurisation des accès aux comptes

Les mots de passe permettant d'accéder aux comptes doivent être sécurisés. A cet égard, il convient d'utiliser des **mots de passe uniques et complexes, régulièrement renouvelés**, et de prévoir une **authentification multifactorielle** afin de mettre en place un barrage complémentaire en cas de divulgation dudit mot de passe.

L'utilisation d'un gestionnaire de mots de passe peut être une bonne idée afin d'attribuer des mots de passe distincts et complexes à chaque application, base de données et services, sans avoir à les mémoriser tous.

Le chiffrement des données

Parce qu'elles se déplacent d'un lieu de stockage à un autre, les données hébergées dans le Cloud risquent davantage d'être interceptées. Aussi, pour les rendre moins vulnérables, différentes façons de chiffrement peuvent être envisagées afin que les communications ne puissent à aucun moment être accessibles aux personnes extérieures sans la clé de chiffrement :

- le **chiffrement de bout en bout** de l'ensemble des données qui sont chargées dans le Cloud (recommandé pour les informations financières, confidentielles ou commercialement sensibles) ;
- le **chiffrement des communications** avec le Cloud dans leur intégralité ;
- **le chiffrement de données particulièrement sensibles,** comme les identifiants de compte **.**

Il est fortement recommandé d'utiliser si possible **ses propres clés de chiffrement** et non pas celles du prestataire.
Il est également très important de gérer les clés de chiffrement de manière **sûre et sécurisée**. Il est ainsi recommandé de les conserver précieusement en dehors du Cloud, au sein même de la structure. Il peut être par ailleurs envisagé de les **mettre à jour régulièrement**.

L'installation des mises à jour de sécurité

Les cybercriminels étant toujours à l'affut des vulnérabilités, il convient de toujours installer au plus vite les mises à jour et correctifs de sécurité.

La vérification de la sécurité du fournisseur de service Cloud

Avec le recours au Cloud computing, la cybersécurité n'est plus seulement de la responsabilité du client mais dépend également du fournisseur de service. Il est donc important de se poser les questions suivantes avant de choisir son fournisseur :

- des audits externes de sécurité sont-ils effectués régulièrement ?
- les données relatives aux clients sont-elles segmentées logiquement et conservées séparément ?
- les données sont-elles chiffrables ? Sont-elles chiffrées ? Quelles sont les parties chiffrées ?
- quelles sont les politiques appliquées en matière de conservation des données des clients ?
- les données sont-elles bien effacées lorsqu'on quitte un service dans le
- Cloud ?
- comment les droits d'accès sont-ils contrôlés ?

Il convient également de lire attentivement les conditions d'utilisation (CGU) établies par le fournisseur et de s'assurer notamment que les données ne sont pas sauvegardées dans des serveurs situés dans des pays ne disposant pas d'un niveau de protection adéquat.

La mise en place de procédures internes

Il convient également d'établir en interne des politiques de sécurité dédiées au Cloud mais également de prévoir des formations de sensibilisation à destination des employés.

Qu'est-ce qu'un Cloud souverain ?
L'inquiétude grandissante en Europe quant à la dépendance croissante des entreprises et institutions vis-à-vis des grands fournisseurs de Cloud américains pousse de nombreux pays à promouvoir des « *Clouds de confiance* », utilisant la technologie des géants américains mais exploités par des sociétés européennes, dans des centres de données situés en Europe. Le Cloud souverain est donc un modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de Cloud sont physiquement réalisés dans les **limites du territoire national** par une entité de **droit national** et en **application des lois et normes nationales**, afin de préserver la sécurité et la confidentialité de ces données. C'est ainsi qu'en 2021, la Principauté de Monaco a lancé son propre Cloud souverain qui s'appuie actuellement sur deux centres de données sur le territoire national, et un centre de données de secours à Luxembourg.