LIVRE BLANC

LE CLOUD ACT

UNE CLARIFICATION POUR TOUS

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

2019 / 2020

EDITION

OUR MEMBERS

+400 M€

TURNOVER

19%

GROWTH

30%

EXPORT
TURNOVER

30%

OF REVENUE
REINVESTED IN
INNOVATION

+2500

EXPERTS
WORLDWILDE

HEXATRUST

CLOUD CONFIDENCE & CYBERSECURITY

EDITO

Le cyberespace va-t-il être entrecoupé de frontières ? L'ancien patron de Google, Éric Schmidt, prédisait en 2018 un internet scindé en deux, l'un chinois et l'autre américain. Avec l'annonce de Google cette année de ne plus collaborer avec Huawei… nous y sommes !

Jean-Noël de GALZAIN
Président HEXATRUST, PDG de WALLIX Group

Et on voit s'y dessiner dans cet espace stratégique une troisième zone d'influence : une sphère digitale occidentale avec un ensemble disparate de pays tiers revendiquant eux aussi une part de l'action (France, Russie, Japon,…).

Alors quelle sphère d'influence voulons-nous bâtir au sein de l'Internet ?

Accepter le CLOUD ACT revient à accepter la suprématie du droit américain sur le nôtre en matière de droit des consommateurs et à perdre peu à peu le contrôle de nos communications et nos données.

Bâtir une sphère numérique Européenne forte permettrait au contraire de porter haut nos valeurs et de protéger la vie digitale de nos concitoyens et de nos entreprises, enfin développer notre industrie et créer de nombreux emplois. Nous avons aujourd'hui la capacité technologique et financière de cette autonomie stratégique.

Avec le RGPD, l'Union européenne s'est dotée d'un texte de référence pour protéger les données personnelles de ses citoyens, érigé en garantie de nos Droits et Libertés Fondamentaux. Ce texte doit être le vecteur de notre modèle civilisationnel et de notre souveraineté dans le numérique !

Sommes-nous capables d'en faire un standard mondial ?

Aujourd'hui, nous avons des choix à faire, avec des enjeux majeurs.

Nous devons porter cette stratégie auprès de nos alliés Européens pour préserver notre souveraineté. C'est déjà le cas avec le Japon, reconnu aux yeux de la Commission européenne comme ayant « un niveau de protection adéquat » au RGPD ; ou encore la Californie, pourtant siège des géants de la Tech qui se dote du CCPA -California Consumer Privacy Act- en vigueur le 1er janvier 2020.

Ensemble, nous pouvons bâtir un espace numérique dans lequel prévalent les droits et libertés fondamentaux de notre société, nos intérêts économiques, nos informations commerciales, industrielles, financières ou techniques, à l'abri des lois extraterritoriales de type CLOUD ACT ou équivalent.

L'Europe a ouvert la voie avec le RGPD, à nous d'en élargir le périmètre et d'en faire un standard mondial.

TABLE DES MATIÈRES

INTRODUCTION

Clarifier, c'est le premier mot de l'acronyme qui constitue le titre de cette Loi votée par le Congrès américain au premier trimestre 2018 : le CLOUD ACT.

Maître Olivier ITEANU
Avocat, VP Hexatrust, Responsable de la Rédaction et Publication du Livre Blanc, CLOUD ACT « Une clarification pour tous »

CLOUD pour Clarifying Lawful Overseas Use of Data, qui peut se traduire par Loi pour clarifier l'usage légal des données hors des États-Unis.

CLOUD est aussi cette technologie constituée de divers services informatiques externalisés. Le cloud est la seconde jambe d'Hexatrust avec la cybersécurité, sa première.

Aussi, au regard de cette Loi qui légalise une sorte de partenariat public – privé américain entre les autorités publiques des États-Unis et les entreprises du numérique américaines, il nous est apparu nécessaire d'apporter notre propre compréhension du texte, car celui-ci peut avoir des effets jusqu'en Europe et en France.

D'abord, parce que nombreuses sont les entreprises européennes qui confient leurs données à un prestataire américain, notamment dans le cadre des services du Cloud Computing.

Ensuite, parce qu'à l'occasion de la sortie surprise de ce texte de Loi, quelques semaines avant l'entrée en application du RGPD [1] le 25 mai 2018, peu nombreux ont été les commentaires sur le CLOUD ACT en France. Pire encore, certains de ces commentaires censés expliquer ce texte de Loi, ne disaient pas toute la réalité du texte. Or, l'association Hexatrust a toujours été ce lieu où la parole a pu librement s'exposer, pour porter nos valeurs et ambitions d'une autonomie numérique européenne.

Il nous appartenait dès lors d'exposer la réalité du CLOUD ACT.

C'est désormais fait au travers de ce livre blanc et je voudrais remercier Alexandra Djateu, Responsable juridique d'IDnomic qui m'a accompagné pour animer ce groupe de travail composé de juristes et non-juristes, représentant les membres de notre association. Cette communauté de compétences au sein d'Hexatrust aboutit à ce travail très « clair » et didactique.

Il revient maintenant à chaque entreprise d'en tirer les conséquences par le choix du bon prestataire numérique à qui elle confie ses données. Elle peut être également organisée de telle façon à ce que la confidentialité des données confiées soit préservée, ou enfin, qu'elle dispose de certaines garanties.

Il ne pourra plus être dit, désormais, qu'on ne savait pas.

Bonne lecture !

1 Règlement Général sur la Protection des Données (Règlement UE n° 2016/679)

LE CLOUD ACT, C'EST QUOI ?

Le CLOUD ACT est une Loi américaine (H.R.4943) votée par le 115ème Congrès américain et promulguée le 23 Mars 2018 par le Président Donald Trump.

Il s'agit d'une **Loi bipartisane** (votée par les Démocrates **et** les Républicains) proposée par le membre républicain du Congrès, **Dog Collins**, ancien Lieutenant-Colonel de l'USA AIR FORCE.

Son titre est un acronyme qui signifie « **C**larifying **L**awful **O**verseas **U**se of **D**ata » pour **CLOUD**.

EXTRA TERRITORIALITÉ

C'est une Loi nationale certes, mais dont les **effets extra-territoriaux** sont affirmés dès le titre (« Overseas » signifie hors des États-Unis) dès lors qu'il existe un **lien suffisant** avec les États-Unis, la loi américaine s'applique.

ACCÈS AUX DONNÉES RENFORCÉ

Le Congrès lui-même résume le texte ainsi : "*To amend title 18, United States Code* to improve law enforcement access to data stored accross borders*".

**il s'agit du principal code pénal du gouvernement fédéral des États-Unis*

LE CLOUD ACT, POURQUOI ?

UN OUTIL AU BÉNÉFICE DES AUTORITÉS AMÉRICAINES

L'objectif premier qui a amené au vote du CLOUD ACT est d'améliorer le travail des autorités d'enquêtes et de poursuites américaines, fédérales ou locales, dans leur quête de données numériques hors des États-Unis.

LUTTER CONTRE LE TERRORISME ET LE GRAND BANDITISME

Améliorer la "*public safety and combat* ***serious crime****, including terrorism*".

La notion de crime étant particulièrement étendue*

Section 2 (1) CLOUD ACT

ACCÈS AUX DONNÉES RENFORCÉ

Texte résumé par la formule utilisée par le Congrès : "*to improve law enforcement access to data stored accross borders*".

* ***Conformément au Code of Federal Regulations Titre 37 § 11.1, « serious crime » signifie :***

(1) toute infraction « criminelle » classée comme un crime en vertu des lois des États-Unis, d'un État ou d'un pays étranger où le crime a été commis ; ou,

(2) toute infraction « criminelle » dont l'un des éléments constitutifs - tel que déterminé par la définition légale ou de common law [2] *- d'un tel crime dans la juridiction où le crime a été commis, comprend l'ingérence dans l'administration de la justice, les faux serments, les fausses déclarations, la fraude, le défaut volontaire de produire une déclaration de revenus, la tromperie, la corruption, le chantage, le détournement, le vol ou une tentative, complicité ou incitation d'autrui à commettre un tel crime.*

2 Système juridique qui se base sur des règles qui sont édictées par les tribunaux et la jurisprudence, par opposition au système de droit civil qui se base sur le droit codifié.

LE CLOUD ACT, POURQUOI ?

UN OUTIL À DESTINATION DES ENTREPRISES AMÉRICAINES

Le CLOUD ACT permet aussi de « clarifier » la position des acteurs numériques américains, lorsque des autorités d'enquêtes et de poursuites de gouvernements étrangers leur demandent la transmission de données numériques.

RÉGULARISER UNE PRATIQUE

Le congrès américain a légalisé un partenariat public/privé, des pratiques déjà en cours et dénoncées par Edward Snowden en juin 2013 dans le Guardian et le Washington post.

FAIRE PRIMER, DE FAIT, LA LOI AMÉRICAINE

Permettre aux acteurs numériques américains de se déterminer sur une demande d'un gouvernement étranger fondée sur sa loi locale, en fonction de leur loi nationale.

MISER SUR LA PRIMAUTÉ DES ACTEURS AMÉRICAINS

En Europe, les GAFAM ont acquis des situations quasi monopolistiques.

Les résidents européens utilisent en masse leurs services. Cela les rend incontournables dans les enquêtes menées par les autorités d'enquêtes et de poursuites (police et justice) européennes pour identifier les auteurs d'infractions.

QUELLES DONNÉES SONT CONCERNÉES ?

L'EXHAUSTIVITÉ DU CLOUD ACT

Le CLOUD ACT permet aux autorités américaines de demander l'accès à toute donnée numérique placée sous le contrôle du fournisseur de service susceptible de les intéresser dans le cadre d'une enquête.

INDÉPENDAMMENT DE LA NATURE DE LA DONNÉE

Les données concernées par le CLOUD ACT : Toutes données (métadonnées et contenus, données personnelles ou non).

"*any record or any information pertaining to a customer or a subscriber* [3]" - Section 3 (a) CLOUD ACT

INDÉPENDAMMENT DE LA NATIONALITÉ DE LA PERSONNE

La nationalité des personnes ciblées par les autorités américaines au travers du CLOUD ACT quelle que soit la nationalité de la personne ciblée et son lieu de résidence.

INDÉPENDAMMENT DE LA LOCALISATION DE LA DONNÉE

Quel que soit le lieu où sont stockées les données concernées par le CLOUD ACT.

"*regardless of whether such communication, record or other information is located* ***within or outside of the United States*** [4]" - Section 3 (a) CLOUD ACT

Le CLOUD ACT est donc en mesure de renforcer l'accès aux données tant qu'elles sont détenues par un fournisseur de services numériques et de cloud.

- Pas seulement les métadonnées ;
- **Tous les contenus**, y compris les courriels ainsi que tous fichiers.

Exemples : Une note stratégique, un document de conception industrielle, une discussion sur une fusion-acquisition, les avis juridiques des juristes d'entreprise portant sur des opérations stratégiques, une base de données de clients soumis au RGPD, une donnée financière et/ou comptable pour une entreprise soumise à une réglementation boursière, etc.

3 Traduction : Tout dossier ou toute information concernant un client ou un abonné.
4 Traduction : Indépendamment du fait que ces communications, enregistrements ou autres informations se trouvent à l'intérieur ou à l'extérieur des États-Unis.

QUELS PRESTATAIRES SONT CONCERNÉS ?

Tous les fournisseurs de services numériques et de cloud sont concernés.

"*a provider of electronic communication services or remote computing service* [5]" - Section 3 (a) CLOUD ACT

QUI & OÙ ?	SOUMIS ?
Fournisseur dont le siège social est établi aux États-Unis	**OUI**
Filiale établie aux États-Unis d'un fournisseur dont le siège social est en Europe	**OUI**
Filiale établie en Europe d'un fournisseur dont le siège social est aux États-Unis	**OUI**
Fournisseur établi hors des États-Unis et sans lien avec les États-Unis	**NON**

5 Traduction : un fournisseur de services de communications électroniques ou de services informatiques à distance.

QUEL CONTRÔLE ET QUELS RECOURS JUDICIAIRES ?

UN CONTRÔLE INCOMPLET OU INCERTAIN

La majorité des injonctions de communication de données en provenance des autorités américaines auront été avalisées par un juge.

> Mais pas toutes, notamment dans le cas des métadonnées (sauf données de géolocalisation).

> Quelle est la réalité du contrôle par le juge ? Le juge va rendre une décision sur la base des seules informations qui lui sont communiquées par les seules autorités publiques américaines, en l'absence de la partie ciblée (pas de contradiction).

DES RECOURS POSSIBLES, MAIS LIMITÉS

Le fournisseur de services cloud qui reçoit une demande pour un citoyen européen pourra la contester devant la justice américaine, si le citoyen européen appartient à un pays qui a conclu un « *executive agreement* [6] », avec l'État américain (à la date de ce jour, aucun accord signé).

> **Mais dans tous les cas,** il n'y a aucun recours prévu pour la personne concernée par la demande de communication de ses données.

L'utilisateur et/ou client du fournisseur de services cloud sera-t-il seulement informé de la demande de communication reçue par celui-ci ? Si on fait savoir au fournisseur de services cloud que cette information peut mettre en danger une enquête en cours, le fournisseur de services cloud ne prendra ni le risque, ni la responsabilité de communiquer à son utilisateur cette demande d'information. L'utilisateur se retrouve donc tributaire de l'attitude adoptée par le fournisseur de services, qui pourra décider d'une part de contester ou non la demande des autorités américaines, et d'autre part de l'avertir qu'il fait l'objet d'une enquête.

Le CLOUD ACT met en place **une nouvelle forme de coopération bilatérale entre les États-Unis et le reste du monde,** État par État, en contournant des mécanismes de droit ; international et internes.

6 Accord bilatéral de coopération entre l'exécutif américain et ses homologues étrangers.

QUEL CONTRÔLE ET QUELS RECOURS JUDICIAIRES ?

Le CLOUD ACT permet un accès réciproque aux données pour les *qualifying foreign states*. Pour être qualifiés, les États doivent être certifiés par l'avocat général et le secrétaire d'État américain (ministre des affaires étrangères américain) comme respectant certaines garanties et notamment des protections procédurales solides pour le respect de la vie privée.

Les *qualifying foreign states*, ayant signé un *executive agreement* avec les États-Unis, seront préautorisés à faire des demandes de communication de données directement auprès des fournisseurs de services plutôt que de passer par le gouvernement américain comme c'était le cas sous l'empire des traités d'assistance mutuelle (*Mutual Legal Assistance treaty* ou MLAT).

Ces *executive agreements* concernent les données de citoyens étrangers, mais excluent les données de citoyens américains dont les demandes de communication devront passer par l'ancien système des MLAT.

Les fournisseurs de services pourront s'opposer aux demandes de divulgation en réunissant la preuve que deux conditions cumulatives sont réunies :

- L'utilisateur n'est pas un citoyen américain ou un résident permanent des États-Unis ;
- La divulgation des informations créerait un risque matériel de violation de la législation d'un gouvernement étranger ayant conclu un *executive agreement* avec le gouvernement américain.

Une fois saisi, aux termes d'une procédure complexe, le juge pourrait annuler ou modifier l'injonction si « une bonne administration de la justice » le commande et si les deux conditions précédentes sont réunies.

Cette « bonne administration de la justice » est elle-même appréciée à travers une « *comity analysis* », c'est-à-dire une analyse de courtoisie internationale, qui consiste à mettre en balance les intérêts des États-Unis et ceux du pays où la demande est faite. Cette balance des intérêts se fait au regard de 8 éléments listés par le CLOUD ACT. Elle permet au juge de prendre en compte certains paramètres pour décider ou non d'appliquer une loi ayant des effets extraterritoriaux.

Dans les cas où aucun *executive agreement* n'est signé il existerait toujours une faculté d'opposition sur le fondement du principe de courtoisie internationale, qui est également reconnu comme principe général de *common law* [7].

7 Système juridique qui se base sur des règles qui sont édictées par les tribunaux et la jurisprudence, par opposition au système de droit civil qui se base sur le droit codifié.

QUELS RISQUES POUR UNE ENTREPRISE EUROPÉENNE ?

UN PARTAGE DES DONNÉES AVEC UN TIERS PEU ENCADRÉ

Le CLOUD ACT impose de donner à un tiers (autorités d'enquêtes et de poursuites américaines) un accès à tous types de données, y compris stratégiques et non nominatives, de surcroît sans garantie sur les conditions de stockage et de conservation en termes de sécurité et de temps.

Le respect des garanties de transferts des données imposé par le Règlement Général sur la Protection des Données (RGPD) n'est pas assuré (cf. articles 44 à 50 du RGPD).

RISQUE D'ESPIONNAGE INDUSTRIEL

Le CLOUD ACT pourrait permettre de donner accès à ses données, directement ou indirectement, à des concurrents. L'espionnage industriel avec ou sans l'intervention des autorités américaines ou défaillance des autorités américaines est un risque concret. Ce sont ici des risques de fuite de données, mais également d'incidents de sûreté.

La conservation des données peut être soumise à un accident, une cyberattaque, une fraude interne ou à un détournement des droits d'accès (ce que le Sénat américain a appelé le LOVINT c'est-à-dire détournement des accès par des agents, par amour ou par intérêts).

> Dans son livre « Data and Goliath » (W. W. Norton & Company – Mars 2015), Bruce Schneier évoque cette pratique illégale, mais qui peut ne pas être sans conséquence pour les personnes ciblées. Citant Edward Snowden et un audit de la NSA réalisé sur 12 mois entre 2011 et 2012, il révèle que cette pratique aurait été relevée durant cette période 2 776 fois sur les traitements de l'Agence nationale de la sécurité rattachée au département de la défense des États-Unis. Il ajoute que le chiffre devrait être bien plus important, car ces informations viennent de la NSA elle-même.

Le risque pour les entreprises européennes serait donc de subir la concurrence déloyale de leurs concurrents américains. Ce risque n'est pas hypothétique quand on examine les chiffres donnés par le rapport parlementaire Gauvain, qui montre que le *Department of Justice* [8] poursuit plus souvent et plus sévèrement les entreprises non américaines que les entreprises américaines, par exemple dans le domaine de la corruption des agents publics étrangers [9].

8 Le DoJ est l'autorité de poursuite judiciaire américaine.
9 Rapport parlementaire du député Raphaël Gauvain, du 26 juin 2019, page 19.

QUELS RISQUES POUR UNE ENTREPRISE EUROPÉENNE ?

RISQUE D'ENGAGEMENT DE LA RESPONSABILITÉ VIS-À-VIS D'AUTRES RÉGLEMENTATIONS

Le CLOUD ACT semble a priori incompatible avec la législation européenne et française sur la protection des données personnelles, en ce qu'il impose un transfert de données depuis le territoire de l'UE vers des autorités étrangères.

Le premier risque est d'engager sa propre responsabilité juridique dans le cadre du RGPD pour les données personnelles ainsi transmises sans base légale (cf. article 48 du RGPD) et/ou sans le consentement des personnes concernées, tant pour un responsable de traitement que pour un sous-traitant.

En effet, l'article 48 précise qu'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant le transfert de données n'est pas suffisante, le transfert doit être fondé sur un accord international.

On pourrait envisager que ces dispositions du RGPD soient invoquées devant les juges américains afin de justifier une requête en annulation ou modification de l'injonction des autorités américaines. Mais il est peu probable que cet argument soit recevable.

Il faut d'ailleurs relever que si le client est une personne morale, la transmission de ses données propres ne constitue pas une violation du RGPD par le fournisseur de services numériques américain, le texte ne protégeant que les données des personnes physiques (article 4 du RGPD).

Le second risque est d'engager sa responsabilité sur le fondement de la Loi n°68-678 dite Loi de blocage qui « *interdit (…) de communiquer (…) à des autorités étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public …* » (Art. 1) de 6 mois de prison et /ou 18 000 € d'amende.

RISQUE D'ERREUR SUR LA PERSONNE CIBLÉE

Mettre en danger les personnes ciblées par les autorités américaines à tort (erreurs, homonymies, poursuites sans fondement), violation du secret des affaires consécutive à l'erreur sur la personne ciblée due à la remontée d'informations.

CAS D'USAGE

CONTEXTE

Prenons l'exemple d'un logiciel de gestion de la relation client ou Customer Relationship Management (CRM) américain présent dans la majorité des entreprises.

Le CRM de l'entreprise procède au transfert de données en dehors de l'Union européenne. Ce transfert nécessite le respect de garanties spécifiques au regard notamment du RGPD. Le CRM étant un fournisseur établit aux États-Unis, il est directement soumis au droit américain et donc au CLOUD ACT.

Le CRM peut apporter certains engagements de conformité :

- Rédaction de Binding Corporate Rules (BCR). Il s'agit d'un code de conduite définissant la politique de l'entreprise en matière de transfert des données personnelles. Cela assure la protection des données transférées depuis l'Union Européenne vers des pays tiers au sein d'une entreprise. Ces BCR sont validés par les autorités européennes de contrôle de la protection des données (dont la CNIL).
- Certification ISO 27001.
- Membre du Privacy Shield. Il s'agit d'une autocertification et d'un engagement au respect des règles en vigueur. Il n'y a pas de réel contrôle par la Federal Trade Commission FTC (CNIL américaine). Pour être membre du Privacy Shield, il faut simplement payer une redevance et s'engager à être conforme aux normes. L'entreprise certifie elle-même sa conformité sans que celle-ci ne soit contrôlée par un organisme extérieur.

Toutefois, le fait d'avoir des BCR, d'être certifié ISO 27001 et d'être membre du Privacy Shield ne garantit pas une conformité au RGPD. Un contrat spécifique doit être conclu avec le CRM afin d'être sûr de faire respecter la réglementation européenne s'agissant du traitement des données, s'assurer de leur lieu de stockage et du temps de leur conservation.

Le CRM peut alors proposer à ses clients la signature d'un Data Processing Agreement concernant la protection des données personnelles. Il s'agit d'un amendement au contrat principal signé avec ses clients visant à se mettre en conformité avec le RGPD, et notamment avec la mention des clauses contractuelles types proposées par la CNIL[10].

Ces éléments de protection cités ci-dessus n'empêcheront toutefois pas l'application du CLOUD ACT en cas de demande des autorités américaines.

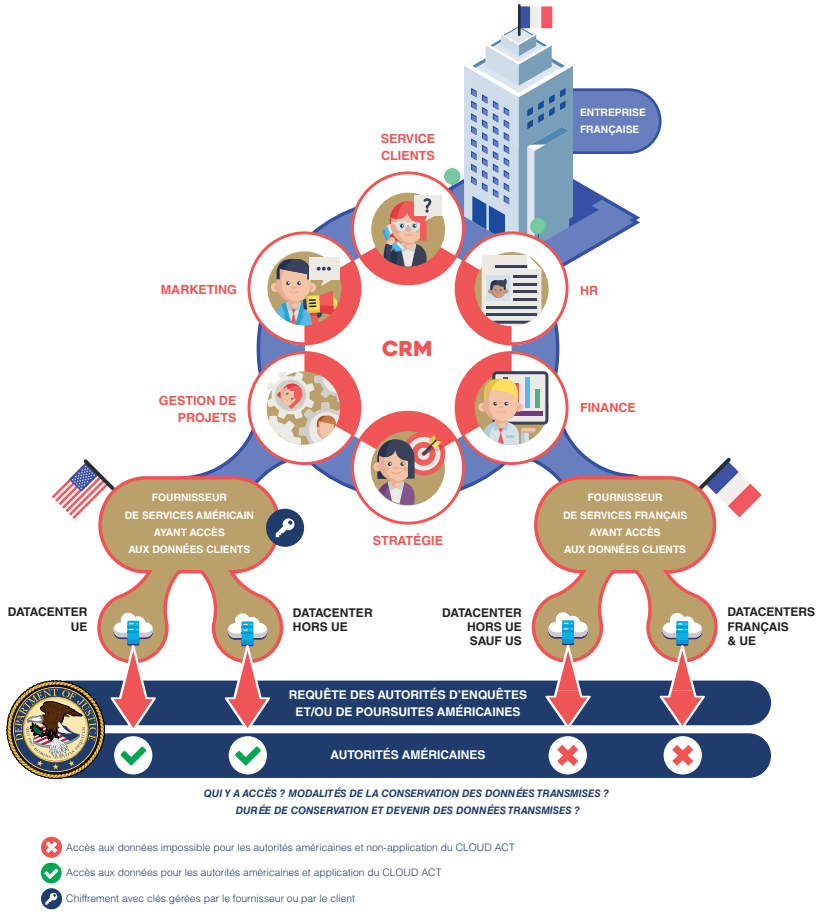
10 Commission Nationale de l'Informatique et des Libertés

SCHÉMA EXPLICATIF ET CONSÉQUENCES

Ci-dessous un schéma comparatif décrivant l'impact d'une demande de transmission des données par les autorités américaines, pour une entreprise française, qui aurait recourt soit :

- à un fournisseur de services cloud américain
- à un fournisseur de services cloud français

Ce schéma reprend l'exemple du Customer Relationship Management CRM ayant accès aux données de l'entreprise française cliente. Il peut s'agir de tout type de données traitées par un CRM, relatives aux ressources humaines, à la gestion de projet, au marketing, à la stratégie, clients finaux de l'entreprise, etc.
La comparaison s'appuie sur la localisation des datacenters hébergeant les données de l'entreprise cliente, au sein ou en dehors de l'Union européenne.



L'entreprise choisissant un fournisseur de services de CRM américain pourra voir ses données transmises aux autorités américaines en application du CLOUD ACT, indépendamment du fait que les datacenters de ce fournisseur de services soient situés au sein ou en dehors de l'Union européenne.

Dans le cas où l'entreprise cliente a recours à un fournisseur de services américain, le niveau de sécurité peut être renforcé en s'assurant que ce soit le client - et non le fournisseur - qui possède les clés de chiffrement.

Deux hypothèses sont possibles :

> Un chiffrement avec clés gérées par le fournisseur : du point de vue du CLOUD ACT, cette option ne présente pas d'intérêt, puisque le fournisseur reste en mesure de communiquer les données clients déchiffrées aux autorités américaines, sur leur requête.

> Un chiffrement avec clés gérées par le client : lorsque les données ne sont pas utilisées, elles sont effectivement chiffrées et le fournisseur n'est pas en mesure de les communiquer de manière déchiffrée aux autorités. Toutefois, pour rendre le service attendu, le fournisseur a besoin que le client lui mette ses clés à disposition, le temps du traitement des données. Même si elles ne sont pas enregistrées chez le fournisseur de services cloud, les clés de chiffrement sont alors présentes en mémoire dans les serveurs et peuvent techniquement être récupérées : cela sera plus ou moins aisé à opérer selon les solutions mises en œuvre (durcissement des serveurs, contrôles d'accès administrateurs renforcés, etc.), mais reste possible, et ainsi ne protège que très partiellement des conséquences du CLOUD ACT.

À noter que même dans l'hypothèse où les mécanismes mis en place seraient suffisamment robustes pour rendre difficile la récupération par le fournisseur des données en clair, il ne peut être exclu que les données puissent être déchiffrées à plus ou moins longue échéance. Subsistera ainsi toujours une suspicion envers la sécurité des données confiées à des fournisseurs soumis au CLOUD ACT : suspicion qui s'attaque aux fondamentaux de la confiance.

Tandis que l'entreprise choisissant un fournisseur de service de CRM français ne pourra voir ses données transmises si les datacenters de ce fournisseur de services sont situés au sein ou en dehors de l'Union européenne, à l'exception évidemment des datacenters situés aux États-Unis.

Dans le cas où le client a recours à un fournisseur de services européen non soumis au CLOUD ACT, s'inscrivant dans une logique de Cloud de confiance ; les données sont sécurisées à la fois :

- du point de vue de l'application du CLOUD ACT et de l'hypothèse d'une requête ;
- vis-à-vis des tiers pour protéger les données sensibles contre la perte, le vol, la publication, l'espionnage, etc. ;
- pour satisfaire aux besoins de souveraineté et de confidentialité conformément à la règlementation en vigueur.

SOLUTIONS ET ALTERNATIVES ?

PRIVILÉGIER L'USAGE DE PRODUITS ET DE SERVICES SOUVERAINS ET DE CONFIANCE

Les sociétés membres d'**HEXATRUST** se distinguent de la concurrence par leur **origine européenne** et leurs solutions **certifiées** et **qualifiées**. La criticité de l'utilisation des solutions de confidentialité rend ces deux points déterminants dans le choix d'une solution.

SÉCURITÉ ET CERTIFICATIONS DE L'ANSSI

Les solutions de cybersécurité et les offres de cloud disponibles sur le marché sont nombreuses et variées, cependant, toutes n'offrent pas le même niveau de sécurité et de confiance. Le respect du référentiel SecNumCloud de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) par les prestataires de services d'informatique en nuage est une garantie du respect de normes de sécurité essentielles.

UN CLOUD DE CONFIANCE

Les éditeurs d'applications SaaS d'HEXATRUST s'engagent d'une part à développer des applications de confiance sécurisées, qui respectent à la fois les règles de « Privacy by Design » et de « Security by Design », et d'autre part à les exploiter dans des Clouds de confiance : des plateformes PaaS, des Infrastructures IaaS, des bases de données DaaS qui respectent l'état de l'art de la fourniture de services Cloud de confiance. Ces entreprises adressent des besoins très divers : solutions collaboratives, postes de travail numériques, sauvegarde des données, plans de reprise d'activités, applications BtoB ou BtoC de toutes sortes qui manipulent des données personnelles ou d'autres données sensibles, mais toujours avec une même vision et un même objectif : assurer la protection et la sécurité des données traitées.

DES FOURNISSEURS DE SERVICES CLOUD SOUVERAINS ET EUROPÉENS

En Europe, les GAFAM ont acquis des situations quasi monopolistiques.

Les résidents européens utilisent en masse leurs services. Cela les rend incontournables dans les enquêtes menées par les autorités d'enquêtes et de poursuites (police et justice) européennes pour identifier les auteurs d'infractions.

Règlement général sur la Protection des Données (RGPD), la Directive Network and Information Security (NIS), le Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur dit règlement eIDAS, etc.

Contractualisation et engagements de l'ensemble des fournisseurs/sous-traitants, structure et organisation réglées par une Politique de Sécurité du Système d'Information (PSSI) à l'état de l'art, gestion rigoureuse des personnels, contrôle interne et respect par les fournisseurs/sous-traitants des réglementations, évaluation continue des risques, information du client sur la localisation de l'hébergement et des données, communication des incidents en conformité avec le RGPD, réversibilité de l'ensemble des données de préproduction, exploitation, sauvegarde... : autant de domaines où les membres d'HEXATRUST font la différence.

CHIFFREMENT & CONFIDENTIALITÉ

En complément de la sécurité offerte en standard par les solutions offertes par leurs fournisseurs, les entreprises ont des besoins de chiffrement sur tous les terminaux et tous les moyens de communication entre ces terminaux. Il faut pouvoir assurer une gestion complète de la confidentialité, proposant une offre sans aucune rupture dans la chaine de confiance.

Les offres d'HEXATRUST couvrent l'ensemble des besoins en chiffrement et peuvent protéger tous types de terminaux, les machines virtuelles (VMs), les outils collaboratifs, les flux de données, l'exécution, le stockage, et même la voix.

Ce niveau de confidentialité des informations peut aussi être renforcé à l'aide d'une clé physique. Acteurs de proximité, les membres d'HEXATRUST s'inscrivent dans des logiques d'excellence techniques, de certification et de souveraineté.

CONTRAT ET CLOUD ACT

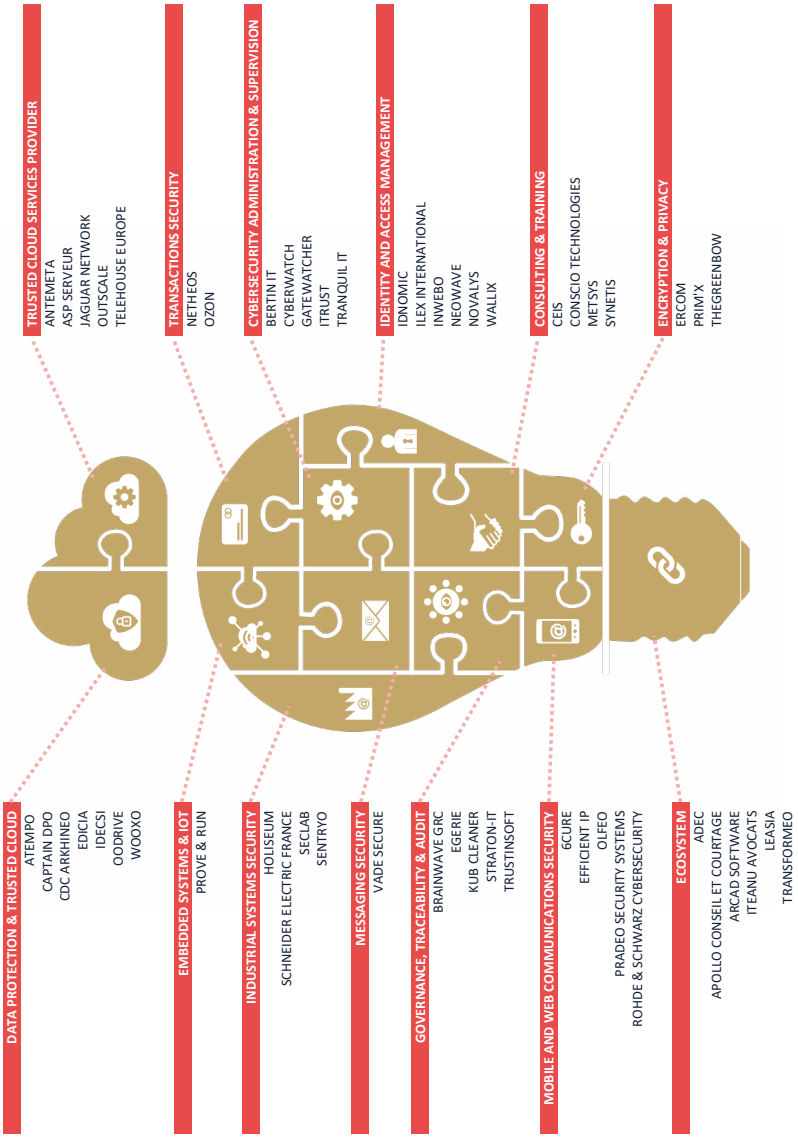
« On ne peut déroger, par des conventions particulières, aux lois qui intéressent l'ordre public et les bonnes mœurs » est un principe posé par l'article 6 du Code civil depuis sa promulgation le 15 mars 1803. Il signifie que le contrat ne peut déroger à l'ordre public. Toute stipulation contractuelle contraire est inopposable aux autorités publiques.

Ce principe français, clairement exprimé dans le Code civil, est universel. Il a donc vocation également à s'appliquer à l'égard des autorités américaines.

Tout fournisseur de Cloud soumis au CLOUD ACT ne pourra opposer aux autorités américaines aucune disposition contractuelle de son contrat avec son client, pour échapper à l'application de la Loi et donc, aux injonctions de communication de données visant ou concernant l'un de ses clients.

CARTOGRAPHIE HEXATRUST

Les solutions des membres HEXATRUST adressent les besoins des utilisateurs en assurant la lisibilité du portefeuille d'offres des membres du groupement.



CONCLUSION

Le CLOUD ACT a surpris, mais cette Loi n'est pas une surprise.

Le CLOUD ACT a été votée prenant au dépourvu les autorités publiques partenaires des États-Unis et au premier chef l'Union Européenne alors que l'on s'affairait au même moment dans toute l'Union à l'entrée en application du RGPD.

Elle a même surpris l'écosystème du numérique, y compris américain, GAFAM en tête. Certains de leurs représentants n'ont pas hésité en public à faire part de leur mécontentement de voir une Loi de ce type, prendre le titre de « CLOUD » identique à leurs offres commerciales éponymes. Mais pour autant, le CLOUD ACT n'est pas tant une surprise, car c'est une nouvelle manifestation d'un processus démarré il y a près de 20 ans.

C'est en Octobre 2001, soit quelques semaines après les attentats du 11 Septembre, que le Congrès votait l'USA Patriot Act, sorte de coup d'envoi d'une surveillance électronique mondiale légitimé par le contexte de l'époque.

En Juin 2013, l'informaticien Edward Snowden révélait les premiers effets de bord de cette surveillance d'un genre nouveau. Le public découvrait l'existence d'un programme d'espionnage gouvernemental appelé PRISM, mis en place par la National Security Agency (NSA) avec la coopération de 11 grandes entreprises américaines. Pour autant et en dépit de ces révélations, rien n'a changé depuis cette date, bien au contraire.

En mars 2018, le Guardian, le New York Times et Channel 4 ont dévoilé une enquête sur une société spécialisée dans le profilage d'électeurs et ont ainsi révélé le scandale Cambridge Analytica où des dizaines de millions de données d'utilisateurs de Facebook avaient été aspirées et auraient servi à des pratiques d'influence aux États-Unis pour la campagne présidentielle de Donald Trump en 2016, mais aussi pour le financement de la campagne du «Leave» pour le Brexit la même année.

Si le Président et fondateur de Facebook a fait le tour du Congrès américain et du Parlement européen pour s'excuser platement devant des caméras, là encore, en pratique rien n'a changé. Le CLOUD ACT est une nouvelle illustration de ce processus.
Quelles économie et protection des mégadonnées souhaitons-nous voir se développer dans le numérique ?

C'est aux gouvernements, notamment européens de réagir et de prendre des mesures pour garantir à la fois la protection des données privées des milliers de citoyens européens et des données stratégiques de nos entreprises.
Pour les entreprises européennes, le problème est entier. Elles se doivent de protéger leurs actifs et leurs données, alors que par ailleurs leur responsabilité juridique au titre de la confidentialité et de la sécurité des données qu'on leur confie s'aggrave.

C'est aussi aux entreprises européennes de faire le choix des fournisseurs de services cloud de confiance dont la prestation répond aux défis de la transformation digitale que nous vivons aujourd'hui et qui s'inscrit dans une logique de certification et de souveraineté.
Nous vivons actuellement avec le CLOUD ACT une situation anormale qui se corrigera sans nul doute un jour. Dans l'intervalle, il faut s'organiser, et prendre notre destin en main, pour que demain, on ne dise plus : « ***CLOUD ACT: what's next?*** »

PUBLICATION

Publication / Conception / Réalisation :

HEXATRUST, Cloud Confidence & Cybersecurity

Responsable de la rédaction et de la publication :

Maître ITEANU Olivier, Avocat, VP HEXATRUST, ITEANU AVOCATS
Depuis 28 ans, Iteanu Avocats développe une activité dédiée au droit numérique.

Rédacteurs :

BEJAT Clémence, Juriste & Data Protection Officer, 3DS OUTSCALE
Fondé en France, en 2010, Filiale et partenaire stratégique de Dassault Systèmes, OUTSCALE fournit des services de Cloud Computing (IaaS) aux organisations privée et publiques souhaitant augmenter leur agilité IT.

DE CHAUVIGNY Vera, Product Marketing Manager, ROHDE & SCHWARZ CYBERSECURITY
ROHDE & SCHWARZ CYBERSECURITY est un leadeur européen de la sécurité informatique qui protège les entreprises et les institutions publiques du monde entier contre les cyberattaques.

DESCORMIERS-THOLLOT Loreline, Chef de projet, HEXATRUST
HEXATRUST est le groupement d'entreprises innovantes des champions du cloud de confiance et de la cybersécurité.

DJATEU Alexandra, Responsable juridique, IDNOMIC
IDNOMIC est le leader européen de la protection et la gestion des identités numériques.

MARTIN GRAEVE Pierre, Service juridique, IDNOMIC
IDNOMIC est le leader européen de la protection et la gestion des identités numériques.

SALGADO Julien, RSSI, JAGUAR NETWORK
Depuis 2001, Jaguar Network a développé une double experise d'hébergement IT sécurisé et d'opérateur de télécommunications très haut débit (THD).

VINCENT François-Xavier, Group CISO & DPO, OODRIVE
Le groupe français OODRIVE propose aux professionnels des solutions de partage, de sauvegarde et de signature électronique répondant aux certifications les plus exigeantes en termes de sécurité.

Design Graphique : **GRONIER Antoine**, HEXATRUST

CONTACT

HEXATRUST, groupement d'entreprises innovantes, est l'alliance gagnante des champions du cloud computing et de la cybersécurité.

Ces pépites technologiques renommées et certifiées partagent les mêmes valeurs et ambitions : Excellence, Confiance, Innovation, Action

Représentatif d'une industrie experte et agile, HEXATRUST propose un panel d'offres et un « **one-stop-shop** » qui répondent aux grands enjeux et aux besoins des organisations publiques ou privées :

- Conformité réglementaire : RGPD, eiDAS, NIS, LPM…
- Protection contre les cybermenaces
- Accompagnement dans les grands projets de transformation digitale

Engagées, les entreprises d'HEXATRUST oeuvrent ensemble pour promouvoir et construire la confiance dans le Cloud et l'excellence Cyber. Dynamiques, elles contribuent au rayonnement numérique français, s'exportent et ambitionnent un essor européen et international.

H E X A T R U S T

CHEZ WALLIX GROUP

250 BIS RUE DU FAUBOURG SAINT-HONORÉ

75008 PARIS

CONTACT@HEXATRUST.COM

WWW.HEXATRUST.COM

@HEXATRUST

H E X A T R U S T

WWW.HEXATRUST.COM