# Faut-il avoir peur du CLOUD Act ?

Précisons tout d'abord que le terme CLOUD Act est en fait l'acronyme de *Clarifying Lawful Overseas Use of Data Act* que l'on pourrait traduire par « Loi pour clarifier l'utilisation légale des données à l'étranger ». En pratique, il s'agit d'un (minuscule) texte de 32 pages glissé incognito dans les quelques 2 232 pages de la loi sur les dépenses 2018 des États-Unis. Ce texte, qui n'a fait l'objet d'aucun débat au Congrès, n'a été médiatisé qu'après sa promulgation par Donald Trump le 23 mars 2018 mettant ainsi l'Europe et le reste du monde devant le fait accompli.

Le CLOUD Act permet de lutter efficacement contre la criminalité au niveau mondial et s'applique dans le cadre d'une procédure pénale suite à un crime ou un délit. Comme toute requête ne doit cibler qu'une personne ou qu'un seul élément identifiant en particulier, le CLOUD Act ne peut (à priori) servir à la réalisation d'opération de surveillance massive comme celles de la NSA révélées par Edward Snowden.

Cette Loi vient combler le vide juridique du Stored Communication Act (SCA) mis en lumière par l'affaire qui opposait depuis 2013 Microsoft à la justice US pour l'accès aux mails d'un présumé trafiquant de drogue stockées en Irlande.

Le CLOUD Act prévoit que les gouvernements étrangers puissent s'engager avec le gouvernement américain par le biais d'accords bilatéraux (executive agreement) afin de « fluidifier » l'accès aux données. Grâce à ce mécanisme et sous réserve que la cible ne soit pas un citoyen américain, l'entraide judiciaire se substitue aux accords d'assistance mutuelle classiques MLAT (*Mutual Legal Assistance Treaty*) dont la lourdeur impose un délai de plusieurs mois pour pouvoir accéder à des données à l'étranger.

La Loi prévoit également qu'un fournisseur US puisse s'opposer dans un délai de 14 jours à une telle demande s'il pense que la personne visée n'est pas un ressortissant américain et que la divulgation l'obligerait à enfreindre la réglementation du pays hébergeant les données. Sa demande sera alors portée devant un tribunal américain qui devra statuer selon les arguments avancés par les deux parties (Police US / Fournisseur US).

Trois questions se posent alors :

- Le CLOUD Act sera-t-il toujours utilisé exclusivement pour lutter contre la criminalité et en aucun cas pour de la surveillance à des fin politiques, stratégiques ou économiques ?
- L'article 48 du RGPD, parfois appelé bouclier Anti NSA, sera-t-il suffisamment protecteur pour empêcher les services américains d'accéder librement aux données

des fournisseurs américains situées au sein de l'UE ?
- L'UE doit-elle s'engager dans ce processus en signant un « executive agreement » avec le gouvernement américain ?

Pour la dernière question, il semble évident que l'Union ne doit pas accepter de signer un accord au terme duquel les Etats-Unis, en raison principalement de l'hégémonie des GAFAM, auraient accès aux données des citoyens européens, quel que soit leur lieu de stockage, tandis que les autorités européennes pourraient seulement accéder à des données stockées aux Etats-Unis en excluant toute donnée concernant des citoyens américains.

La seule attitude possible pour l'Union européenne, dans un souci de réciprocité et de juste équilibre entre la nécessité de la lutter contre la criminalité et la protection des citoyens européens serait de négocier avec les Etats-Unis un accord par lequel les autorités de chaque pays auraient accès de manière fluide aux données nécessaires à la lutte contre la criminalité, et à elles seules uniquement, sans considération de  leur lieu de stockage et sans discrimination sur la nationalité des personnes ou des entreprises concernées.

---

# Les points clés du RGPD

Le nouveau règlement européen pour la protection des données personnelles (RGPD) entrera en application le 25 mai 2018. Ce règlement concerne tous les organismes (publics ou privés) qui traitent des données à caractère personnel de citoyens européens même si le traitement ne s'opère pas sur le territoire de l'union. A moins de trois mois de la date fatidique, nous vous proposons une synthèse, en vidéo, des points essentiels à retenir de ce règlement.

---

# Retour sur la cyberattaque Wannacry


Le 12 mai dernier, une cyberattaque dénommée « Wannacry » défrayait la chronique. Dans cette présentation vidéo, je vous décris le fonctionnement de Wannacry et vous explique le lien avec les failles de sécurité Windows et les outils de la NSA ainsi que le rôle joué par le groupe de hackers « The shadow brokers ».  Enfin, j'évoque quelques bonnes pratiques et les enseignements que l'on peut tirer de cette cyberattaque quelque peu surmédiatisée.

---

# Le référentiel ANSSI SecNumCloud

Le référentiel de qualification des prestataires de services d'informatique en nuage (SecNumCloud) vient enfin d'être publié par l'ANSSI. Qu'apporte t-il par rapport à une certification ISO 27001 ? Donne t-il toutes les garanties de sécurité attendues par les clients ? Nous vous proposons une analyse détaillée de ce référentiel avec en particulier un focus sur 50 exigences. Au-delà de la qualification des prestataires, découvrez comment SecNumCloud peut vous permettre d'évaluer la sécurité de vos fournisseurs.

---

## Sommaire de la présentation

1. Historique du référentiel
    - De la version 1.3 à la version 3.0
2. SecNumCloud v3.0 et les normes ISO relatives au cloud
    - Normes ISO/IEC : 17788, 17789, 27017 et 27018
3. Focus sur 50 exigences pour les prestataires (CSP)
4. Zoom sur 4 recommandations pour les commanditaires (clients)

    - + 2 recommandations importantes additionnelles
5. Conclusion
    - Le référentiel SecNumCloud est-il pertinent ?
    - Quel usage peut-on en faire en tant que CSP ?
    - Quel usage peut-on en faire en tant que Client ?

---

La vidéo d'environ 45mn ainsi que les slides de la présentation sont réservés aux membres enregistrés sur le blog. N'hésitez pas à vous inscrire gratuitement ou utiliser votre compte LinkedIn, Google, Microsoft, Twitter ou Facebook pour pouvoir y accéder.
Pour les personnes non inscrites, un extrait de la présentation est disponible ici.

---


Les slides de la présentation

---

# Privacy Shield : Bouclier ou passoire pour les données européennes ?

Suite à l'invalidation du Safe Harbor par la CJUE le 6 octobre 2015 (voir à ce sujet notre article La CJUE invalide le Safe Harbor), la Commission européenne a adopté le 12 juillet 2016 une décision d'adéquation visant à reconnaitre au mécanisme « EU-U.S. Privacy Shield » (bouclier de protection des données UE-États-unis) un niveau de protection « *équivalent* » aux exigences européennes. Ce nouvel accord a pour effet d'autoriser les transferts de données à caractère personnel depuis l'Union européenne vers les entreprises établies aux Etats-Unis utilisant ce dispositif.

Afin de garantir la conformité aux exigences de l'europe en matière de traitement

des données, l'accord définit des « Privacy Shield Principles » auxquels les entreprises se doivent d'adhérer et de respecter. Toute entreprise qui viole ces principes peut être sanctionnée et doit mettre fin à l'utilisation des données collectées.

Le Privacy Shield constitue une réelle avancée dans la protection des données européennes en prenant en compte les recommandations formulées par la Commission européenne en novembre 2013 mais également certaines exigences énoncées par la CJUE dans son arrêt du 6 octobre 2015. Pour avoir une vue d'ensemble des principales nouveautés de ce dispositif, on pourra consulter la FAQ publiée par la Commission européenne le 12 juillet.

Selon Maximilien Schrems, citoyen européen à l'origine de l'invalidation du Safe Harbor, « *le bouclier Vie privée est le produit de la pression des États-Unis et de l'industrie des technologies et non le fruit d'une démarche rationnelle ou de considérations raisonnables. Il est un peu plus qu'une petite mise à jour de Safe Harbor, mais non un nouvel accord* ».

Voici les principaux reproches que l'on peut formuler à cette décision d'adéquation :

- Tout comme le Safe Harbor, le principe de certification est déclaratif basé sur le principe de l'auto-régulation. En d'autres termes, pour collecter des données européennes, les entreprises américaines n'ont qu'à s'auto-proclamer « *Privacy Shield Compliant* ». Et bien évidemment la liste des entreprises certifiées est déja longue.
- Le Privacy Shield n'interdit pas l'accès au contenu des communications par les services de renseignement américains. Bien sûr dans le texte, il n'est pas question de parler de « surveillance de masse » mais plutôt de « collecte ciblée ». Dans sa rédaction actuelle, le Privacy Shield ne semble pas respecter l'arrêt de la CJUE du 6 octobre 2015 considérant que la collecte effectuée par l'administration des États-Unis était contraire à la Charte des droits fondamentaux de l'Union européenne.
- Pour répondre aux exigences de la CJUE et du G29, un médiateur (Ombudsman) est chargé de traiter les plaintes de tout citoyen européen qui conteste un traitement ou une surveillance illégale. Mais quelle peut-être l'indépendance de ce médiateur dès lors qu'il est nommé par le Secrétaire d'État américain ? D'autre part, le médiateur ne pourra ni confirmer ni infirmer que les États-Unis se sont livrés à une surveillance du plaignant. L'ombudsman devra conclure en disant si les lois américaines ont été respectées ou que le problème de non-conformité a bien été résolu. Naturellement, aucune institution européenne ne sera habilitée à inspecter les Datacenters ou les logiciels américains. Dans ces conditions, le plaignant n'aura strictement aucun regard possible sur la réalité de la surveillance effectuée.

- Le Privacy Shield ne se substitue pas aux deux alternatives actuellement en vigueur que sont les clauses contractuelles types (EU model clauses) ou les règles internes d'entreprises (BCR). En conséquence, si une entreprise couverte par le Privacy Shield s'en fait exclure pour non-respect des obligations, elle pourra quand même continuer à traiter les données via l'un des deux mécanismes précédemment cités.
- La conservation des données n'est pas limitée dans le temps. Les sociétés américaines peuvent donc utiliser les données aussi longtemps qu'elles le souhaitent tant que cela sert l'objectif pour lequel elles ont été initialement collectées ou ultérieurement autorisées.
- Même si une révision annuelle est prévue, il parait surprenant que l'accord porte uniquement sur les exigences de la Directive 95/46/EC alors même qu'un nouveau règlement européen  plus contraignant entrera en vigueur le 25 mai 2018 et abrogera la directive de 1995. Pourquoi n'a t-on pas prévu une clause de suspension afin de prendre en compte les exigences du nouveau règlement dans un nouvel accord UE/US ? Pourquoi la Commission européenne veut-elle alourdir les contraintes réglementaires sur les entreprises européennes alors que dans le même temps elle semble se satisfaire des promesses des sociétés américaines ?

Compte tenu des réserves que nous venons d'évoquer, il n'est pas impossible de voir le Privacy Shield faire l'objet d'un recours devant la CJUE, seule compétente pour constater la validité d'un acte de l'union conformément à l'article 263 du Traité sur le fonctionnement de l'Union européenne (TFUE).

---

# 10 recommandations pour maîtriser les risques dans le Cloud

Le Cesin (Club des Experts de la Sécurité de l'Information et du Numérique) en collaboration avec la CNIL, l'ANSSI et des juristes spécialisés vient de publier 10 recommandations pour maîtriser les risques dans le Cloud computing. Chez Verisafe, nous travaillons sur la sécurité du Cloud depuis plus de 6 ans et nous avons créé la méthodologie EFICAS (Evaluation Formelle et Indépendante du Cloud pour l'Adopter en toute Sécurité) destinée justement à maîtriser les risques dans le Cloud. Il nous est donc apparu intéressant d'analyser et de commenter les 10 recommandations du Cesin et de faire le lien éventuel avec notre méthodologie EFICAS.

---

**Recommandation 1 :** Estimez la valeur des données que vous comptez externaliser ainsi

que leur attractivité en termes de cybercriminalité.

Comment estimer la valeur de nos données ? Quel sont les critères de valorisation ? Il s'agit ici de classifier les données que l'on souhaite externaliser. En pratique, cette classification dépendra du type de données utilisées. Pour des données de bureautique, elle peut être relativement simple comme par exemple une classification sur 5 niveaux basée sur deux critères : confidentialité et conformité.

| Niveau | Désignation | Commentaires |
|---|---|---|
| 1 | Usage Interne | Accessible à l'ensemble du personnel |
| 2 | Réglementé CNIL (DCP) | Fait l'objet d'une règlementation en vigueur |
| 3 | Réglementé ASIP (DSCP) | Fait l'objet d'une règlementation en vigueur |
| 4 | Confidentiel entreprise | Droits d'accès approuvés par la hiérarchie |
| 5 | Stratégique entreprise | Acccès limité à une groupe de personnes |
| | | *EFICAS - © Copyright 2016 VERISAFE S.A.S* |

Mais pour d'autres projets Cloud, ce type de classification peut s'avérer totalement inadapté. Par exemple, dans un projet IoT où les objets connectés remontent des informations dans le Cloud, les critères de disponibilité et d'intégrité seront sans doute plus pertinents. Prenons l'exemple de sondes thermiques qui remontent des valeurs de température dans le Cloud. Ces données ne sont à priori pas confidentielles ni réglementées mais leur altération ou leur indisponibilité pendant une longue durée  peut s'avérer critique. Dans la méthodologie EFICAS, nous préconisons de classifier toutes les données que l'on souhaite héberger dans le Cloud. Pour cela, nous avons développé une grille modulaire permettant de classifier facilement tout type de données qu'il s'agisse de données issues d'un SI classique, d'un réseau industriel ou du monde de l'Internet des objets.  Dans notre méthodologie, la classification des données n'est pas une étape strictement obligatoire mais elle permet, lorsqu'elle est réalisée, d'industrialiser le processus EFICAS pour un ensemble de projets.

---

**Recommandation 2 :** S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la DG le principe de leur externalisation

Sur le principe, cette recommandation tombe sous le bon sens mais en pratique, c'est quoi une donnée sensible ou une donnée stratégique ? Une DCP (Donnée à caractère personnel), c'est une donnée sensible ? La propriété intellectuelle dans le projet X c'est sensible ou stratégique ? Les données commerciales de l'agence Y, c'est sensible ? Au final, il sera difficile de savoir à quel moment et pour quel type de données, il convient d'obtenir une aval de la DG. Dans la méthodologie EFICAS, nous considérons qu'une validation par la DG est importante mais il ne s'agit en aucun cas de valider le principe de l'externalisation mais uniquement de valider les

écarts entre risques tolérés par l'organisme et risques dans le Cloud après avoir epuiser tous les recours traditionnels de réduction des risques.

Concernant l'attractivité de vos données en termes de cybercriminalité, il s'agit effectivement d'un élément important qui permettra d'établir un niveau de menace sur vos données. Si vous stockez dans le Cloud des données sans aucun intérêt pour un concurrent, une agence de renseignement ou un cybercriminel, la faible attractivité de vos données entrainera un faible niveau de menace. Par contre, si vous stockez dans le Cloud des données de propriété intellectuelle stratégiques ou les numéros de carte bancaire de vos clients, l'attractivité sera radicalement différente et donc le niveau de menace bien plus élevé. Ce niveau de menace sera utile dans le processus d'analyse de risque lorsqu'il s'agira d'évaluer la probabilité d'occurrence des incidents de sécurité.

---

**Recommandation 3 :** Evaluez le niveau de protection de ces données en place avant externalisation.

C'est un élément également pris en compte dans la méthodologie EFICAS. En effet, le niveau de protection des données mis en œuvre dans l'organisme donne une première indication sur l'importance que l'entreprise accorde à ces données. Par exemple, le fait que les données soient stockées en clair (non chiffrées) et accessibles à un très grand nombre d'utilisateurs traduira sans doute une faible sensibilité de ces données en terme de confidentialité. Il s'agira alors de vérifier que dans le Cloud les données sont aussi bien, voire mieux protégées qu'en interne dans votre entreprise.

---

**Recommandation 4 :** Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offre en fonction du résultat du point 1.

Les exigences de sécurité peuvent effectivement être définies selon la valorisation des données issues de l'étape 1 mais également de l'étape 3. Il est en effet assez courant d'être beaucoup plus exigeants sur le niveau de sécurité d'une prestation externalisée que sur le même type de prestation réalisée en interne. Reste à savoir si ces exigences plus fortes vis-à-vis du prestataire sont justifiées. Dans la méthodologie EFICAS, plutôt que de partir sur des exigences de sécurité souvent difficiles à établir et à valoriser, nous démarrons le processus sur la base d'une cartographie des risques établis spécifiquement pour le Cloud computing. L'étape initiale consiste pour l'organisme à définir son niveau de tolérance pour chaque risque identifié.

---

**Recommandation 5 :** Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc. Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise.

Une analyse de risque constitue bien évidemment une approche pertinente mais ici le Cesin n'identifie qu'une dizaine de risques et ne donne aucune indication pour les traiter. La méthodologie EFICAS établit une cartographie exhaustive des risques dans le Cloud (42 risques) et propose un arsenal complet de mesures spécifiquement adaptées aux problématiques dans le Cloud (CCM v3 de la CSA, ISO 27017 de l'ISO, contrat de cyber-assurance, …).

Après avoir sélectionné les risques pertinents dans le catalogue, Il faut ensuite être en mesure d'évaluer son propre niveau de tolérance aux risques. Dans un deuxième temps, il faut évaluer le niveau réel des risques dans le projet Cloud envisagé. La méthodologie EFICAS fournit aux entreprises tous les livrables nécessaires à la réalisation de ces deux étapes particulièrement délicates.

---

**Recommandation 6 :** Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée.

« Exigez », c'est vite dit ! Demandez donc à Amazon, Google ou Microsoft un audit de sécurité sur leur infrastructure Cloud public. La réponse sera toujours négative. Vos exigences n'étant pas acceptées, que faire maintenant ? En pratique, la recommandation du Cesin n'est quasiment jamais applicable dans le cas d'un Cloud public. C'est la raison pour laquelle la méthodologie EFICAS propose une approche radicalement différente pour évaluer le niveau de sécurité du prestataire.

---

**Recommandation 7 :** A la réception des offres analysez les écarts entre les réponses et vos exigences.

Comme on vient de le voir à l'instant, on ne peut que rarement recourir à l'audit

dans un Cloud public. Pour l'organisme client, il sera  donc impossible de vérifier l'adéquation du niveau de sécurité du prestataire avec ses exigences. Comme indiqué lors de la recommandation (4), la méthodologie EFICAS permet d'établir une grille de tolérance aux risques plutôt qu'une liste d'exigences. Puisque l'audit n'est pas possible, EFICAS définit une liste d'évaluation des risques auquel l'organisme s'exposera dans le Cloud. Il suffira ensuite de contrôler les écarts entre risques tolérés par l'organisme et risque exposés dans le projet Cloud et de traiter les risques inacceptables avec les mesures spécifiquement adaptées au Cloud (CCM v3, ISO 27017, ISO 27018, assurance, …).

---

**Recommandation 8 :** Négociez, négociez.

Dans le Cloud et contrairement aux contrats d'infogérance classique les négociations avec le fournisseur sont assez limitées et parfois même inexistantes. On constate en effet aujourd'hui un déséquilibre de rapports de force entre les entreprises clientes et les fournisseurs. Ces derniers proposent le plus souvent des contrats standards non négociables. Pour bien comprendre cette difficulté, on peut citer l'expérience réelle d'une grande entreprise française du CAC 40 qui souhaitait négocier de nouvelles clauses de sécurité avec Google Inc. au lendemain des révélations d'Edward Snowden. Après de multiples tentatives y compris un rendez-vous avec la direction au siège social de Google France à Paris, le fournisseur américain a rejeté toutes les demandes du client et n'a en conséquence modifié aucune clause contractuelle. Face à Amazon, Google, Salesforce ou Microsoft, le rapport de force est souvent à l'avantage des fournisseurs américains même pour une grande entreprise cliente. Il va sans dire que les possibilités de négociation sont encore plus hypothétiques pour une PME ou une collectivité territoriale.

---

**Recommandation 9 :** Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.

Cette recommandation ne pose généralement pas de problème aux fournisseurs. Attention cependant à ne pas tomber dans l'excès comme l'ANSSI l'a fait dans son référentiel de qualification de prestataires de services sécurisés d'informatique en nuage. Si l'on suit les exigences de l'agence (localisation  des données exclusivement sur le territoire français, support de premier niveau francophone localisé en France, contrat de droit français, tribunal compétent français), on risque fort de se retrouver devant une offre Cloud extrêmement limitée qui ne répondra pas aux attentes des métiers.

**Recommandation 10 :** Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

On entre encore ici dans une difficulté particulière du Cloud, le contrôle de la sécurité. Comme le Cesin le sous entend en précisant « si cela est possible », les audits ne sont généralement pas admis sur une infrastructure Cloud public. Les fournisseurs acceptent plus souvent les tests d'intrusion (sur un périmètre précis) mais leur intérêt est extrêmement limité pour ne pas dire quasi nul. L'approche pragmatique de la méthodologie EFICAS permet de vérifier le niveau de sécurité du fournisseur même lorsqu'un audit n'est pas réalisable. La vérification est basée sur un questionnaire spécifique transmis au fournisseur. Elle est complétée par un contrôle approfondi des certificats de sécurité (ISO 27001, CSA STAR, ISAE3402, Privacy Shield, etc…).

D'autre part, la méthodologie EFICAS met l'accent sur le contrôle continu de la sécurité pendant toute la durée du contrat. Elle établit une liste de contrôles et une description détaillée de chaque paramètre de sécurité, ce qu'il faut mesurer et comment le mesurer. Parmi les paramètres de sécurité, on trouve par exemple la disponibilité du service, la réponse aux incidents, la gestion du cycle de vie des données, la conformité réglementaire, la gestion des vulnérabilités, le chiffrement des données, etc..

---

# Numergy c'est fini

Après une mise sous procédure de sauvegarde le 13 octobre dernier, SFR vient de procéder au rachat de l'intégralité du capital de Numergy. Dans un communiqué de presse publié hier, Michel Combes, PDG de SFR déclare : *« Ce rapprochement s'intègre à la stratégie Entreprise du groupe Altice dont l'une des priorités est de consolider l'ensemble de ses activités autour du Cloud, de l'IOT et des services managés. »*

Il faut se rappeler le projet de Cloud souverain français (Andromède) émane d'un appel d'offres lancé en 2010 dans le cadre des « investissements d'avenir » et que pour des raisons essentiellement politiques, il a donné naissance à deux sociétés Cloudwatt et Numergy. La fin de Cloudwatt est actée depuis un an (rachat par Orange), c'est donc maintenant au tour de Numergy de subir le même sort. Mais pouvait-il en être autrement ?

Dans cette affaire de Cloud souverain beaucoup d'erreurs ont été commises. Celles du gouvernement français tout d'abord. On ne peut en effet que s'interroger :

- Pourquoi financer deux startups concurrentes sur un même marché ?
- Comment peut-on imaginer qu'avec un capital de 225 M€ non entièrement libéré, un nouvel entrant puisse rivaliser face à des géants américains déjà opérationnels et qui continuent leurs investissement à coup de milliards d'euros ?
- Pourquoi n'y a-t-il eu aucune volonté politique pour instaurer une véritable dynamique Cloud auprès des administrations et collectivités locales à l'image du Cloud first Policy instauré aux états-unis ?
- Pourquoi ne pas raisonner à l'échelle européenne avec des produits de sécurité exclusivement européens ou open source afin de revenir un tant soit peu vers la notion de souveraineté ?

Bien sûr Numergy a également commis des erreurs sur le plan commercial, marketing et technologique mais dans un contexte pareil, comment leur en vouloir ? Qui aimerait travailler dans une société dans laquelle les 3 principaux actionnaires ne s'entendent pas, n'ont pas les mêmes intérêts ni les mêmes objectifs et n'ont pas la même vision stratégique du business ?

Pourtant en matière de sécurité, Numergy avait fait beaucoup d'effort. On peut citer par exemple :

- Une excellente redondance via 5 datacenters Tier 3 situés en France,
- Une offfe « Numergy Santé » agrée officiellement par l'état en tant qu'hébergeur de données de santé (HDS),
- Une certification ISO 27001:2013 délivrée par le BSI,
- Une certification CSA STAR Silver délivrée également par le BSI.

Comme quoi dans le Cloud, la sécurité est une condition nécessaire (et même indispensable) mais pas suffisante pour s'imposer sur le marché. Le rachat de Numergy signe ainsi la fin des ambitions de l'Etat français dans son projet de Cloud souverain. Reste maintenant à savoir ce que le groupe Altice va faire de cette activité Cloud.

---

# La Directive NIS sur les rails pour 2016

A l'issue d'une consultation publique (23 juillet – 15 octobre 2012), la commission Européenne a élaboré puis adopté le 7 février 2013 la proposition d'une nouvelle

directive pour la sécurité des réseaux et de l'information. La directive NIS (Network and Information Security) a pour objectif de renforcer la réactivité des 28 États membres et de stimuler la coopération entre les autorités de lutte contre la cybercriminalité, tout en leur donnant des moyens techniques et légaux appropriés.

Approuvée par le Parlement Européen le 13 mars 2014 (521 voix pour, 21 voix contre), la directive NIS prévoit des mesures de sécurité à respecter pour les opérateurs de services essentiels mais également pour les acteurs du marché du numérique. Ces derniers étant définis à l'annexe II du document original de la directive : Plateformes de commerce électronique, Passerelles de paiement par internet, Réseaux sociaux, Moteurs de recherche, Services informatiques en nuage, Magasins d'applications en ligne.

Le 7 décembre 2015, les députés européens ont conclu un accord avec le Conseil pour arrêter le texte final de cette directive. Concrètement, l'accord a permis de finaliser la liste des sociétés concernées par la directive à savoir les infrastructures critiques (appelées OIV en France) mais également les acteurs du marché du numérique pour lesquels les réseaux sociaux sont finalement exclus. Les obligations des acteurs du marché sont beaucoup moins contraignantes que pour les OIV et concernent principalement le signalement obligatoire des incidents de sécurité aux autorités nationales compétentes.

En France, cette obligation n'est pas nouvelle. En effet suite à l'adoption du Paquet Télécom et l'ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques, les opérateurs télécoms ont déjà l'obligation d'informer les autorités nationales compétentes (ici la CNIL) des fuites de DCP (données à caractère personnel). Concernant les opérateurs d'importance vitale (OIV), des obligations de sécurité sont imposées depuis la loi de programmation militaire (LOI n° 2013-1168 du 18 décembre 2013). Ainsi, selon l'article L1332-6-1 du code de la défense : *« Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation.»* Concernant les incidents de sécurité, l'article L1332-6-2 précise que les OIV doivent informer sans délai les services du Premier ministre (l'ANSSI) des incidents affectant le fonctionnement ou la sécurité des systèmes d'information. Des arrêtés sont en cours de finalisation pour définir précisément les modalités selon les secteurs concernés. Pour des raisons de sécurité, certains de ces arrêtés ne seront pas publiées.

Pour pouvoir entrer en vigueur, la Directive NIS devra encore être approuvée formellement par la commission du marché intérieur du Parlement le 14 janvier 2016 puis par le comité des représentants permanents du Conseil. Il s'agira ensuite pour

chacun des 28 États membres de transposer la directive dans leur droit national respectif.

---

# AWS : « surprenante » certification ISO 27017

Chad Woolf, Directeur risques et conformité chez AWS, a déclaré le 30/11/2015 sur le blog officiel d'Amazon : "*I am happy to announce that AWS has achieved ISO 27017 certification*".

Cette annonce est pour le moins surprenante car contrairement à l'ISO 27001, la norme ISO 27017 ne décrit pas un processus de gestion mais fournit un guide de bonnes pratiques. Elle a été développée par l'ISO pour compléter le guide initial définie par l'ISO 27002 et propose un ensemble de mesures de sécurité destinées à améliorer la sécurité des services dans le cloud.

En pratique, AWS a réactualisé son SMSI (pierre angulaire de l'ISO 27001) et mis à jour sa DdA (Déclaration d'Applicabilité) en adoptant les bonnes pratiques de l'ISO 27017. AWS a ensuite demandé à Ernst & Young de procéder à un nouvel audit pour attester de la prise en compte de l'ISO 27017 dans sa démarche ISO 27001.

On peut ainsi lire dans le certificat 27017 d'AWS : *" … certified under certification number [2013-009], is also compliant with the requirements as stated in the standard : ISO/IEC 27017:2015 "*
(*pour information, le numéro de certification [2013-009] correspond au certificate ISO 27001 d'AWS)*

En d'autres termes, Ernst & Young atteste que le SMSI d'AWS prend en compte les bonnes pratiques issues de l'ISO 27017 ce qui n'apporte en soi aucune information précise sur le niveau de sécurité effectif du fournisseur. En effet, en l'absence de publication de la DdA, on ne sait strictement rien sur la façon dont les mesures de sécurité proposées par l'ISO 27017 sont réellement implémentées au sein du SMSI d'AWS. Il s'agit donc encore une fois d'une démarche purement marketing, destinée à rassurer le client perdu dans la jungle des normes ISO/IEC 270xx. Dans le même état d'esprit, AWS aurait pu également demander à Ernst & Young un certificat ISO 27002 puisque naturellement son SMSI s'appuie sur des mesures issues de l'ISO 27002. Et pourquoi ne pas demander dans la foulée un certificat ISO 27005 puisque l'analyse de risque effectuée par AWS s'appuie sur ce référentiel ?

# La CJUE invalide le Safe Harbor



## Qu’est-ce que le Safe Harbor ?

Le « Safe Harbor » (en français sphère de sécurité) est un ensemble de principes de protection des données personnelles, publié par le Département du Commerce américain, auxquels des entreprises établies aux Etats-Unis adhèrent afin de pouvoir recevoir des données en provenance de l’Union européenne. Ces principes, négociés entre les autorités américaines et la Commission européenne, sont essentiellement basés sur ceux de la Directive européenne 95/46 du 24 octobre 1995. Le 26 juillet 2000, la Commission Européenne a adopté une décision d’adéquation qui reconnaît que les principes de « Safe Harbor » assurent une protection adéquate pour les besoins des transferts de données à caractère personnel depuis l’Union Européenne. En conséquence, le transfert des données personnelles de l’UE vers les USA est légal dès lors que l’entreprise américaine est certifiée. La liste des entreprises certifiée (U.S.-EU SAFE HARBOR LIST) est disponible sur le site du département du commerce américain et recense à l’heure actuelle 5482 sociétés.

## Pourquoi cet accord était-il fortement critiqué ?

Tout a commencé avec le Patriot Act., la loi anti-terroriste promulguée le 26 octobre 2001 en réponse aux attentats du 11 septembre. En donnant de très larges pouvoirs aux services de renseignement avec les NSL (National Security Letters) via une législation dérogatoire, le Safe Harbor ne pouvait plus garantir la confidentialité des données hébergées auprès de sociétés de droit américain ou de leurs filiales. En juin 2013, les révélations d’Edward Snowden n’ont fait que confirmer les programmes (PRISM, Xkeyscore,…) d’espionnage de masse des européens avec la collaboration active des leaders américains de l’Internet (Facebook, Microsoft, Apple,…). Si les européens avaient bien connaissance des lois (FISA, Patriot Act) qui permettent aux autorités américaines d’accéder à leurs données personnelles pour assurer la sécurité nationale du pays, ils n’imaginaient pas que les Américains s’en serviraient pour établir une surveillance à des fins économiques

et géopolitiques. D'autre part, le secret autour des activités des services de renseignement relevant du gouvernement américain empêche toute vérification du respect des principes de la Directive Européenne (95/46) notamment sur les activités de recueil, de traitement, de conservation des données et empêche tout contrôle des intéressés sur ces activités.

Pour sa certification l'entreprise américaine peut faire appel à un tiers ou contrôler elle-même qu'elle se conforme aux exigences du Safe Harbor. C'est donc le principe de l'auto-évaluation (self-assessment) qui sera retenue par la plupart des entreprises américaines. Même si l'entreprise doit renouveler sa certification chaque année (selon le même principe), il apparait clairement que de nombreuses sociétés inscrites sur la liste des entreprises certifiée n'ont fait que s'auto-proclamer « Safe Harbor Compliant » en ne respectant en aucune manière les exigences réelles du Safe Harbor. D'autre part, le contrôle du programme étant exclusivement assuré par la Federal Trade Commission, les CNIL européennes (G29) n'ont aucun moyen de contrôler (et encore moins de sanctionner) les entreprises américaines contrevenantes.

## Pourquoi la CJUE a-t-elle été saisie ?

L'affaire démarre en 2011 lorsque un jeune étudiant autrichien de 24 ans, Maximilian Schrems, reproche à Facebook de violer les lois européennes sur la protection des données personnelles. Dans un entretien à Pixels en août 2014, Max Schrems déclare :

« J'assistais à une conférence aux Etats-Unis  et quelqu'un de Facebook est venu nous expliquer comment les lois européennes sur la vie privée fonctionnaient. J'étais le seul Européen. Et il disait : "Vous pouvez faire ce que vous voulez, rien ne vous arrivera jamais". Il interprétait la loi européenne d'une façon qui était complètement fausse. Il disait des choses comme : "*Tant que personne ne vous dit non, vous po*uvez continuer à utiliser l*eurs données".* »

*Max Schrems en janvier 2012. DIETER NAGL / AFP*

Il décide alors de porter plainte contre Facebook à Dublin là où se situe le siège européen du géant américain. En première instance, la justice irlandaise rejette sa demande en considérant que le transfert des données vers les datacenters américains de Facebook étaient couverts par le Safe Harbor. Devenu avocat, et suite aux révélations de Snowden en juin 2013, Schrems ne lâche pas l'affaire et décide de faire appel. Pour prendre sa décision, la High Court of Ireland (Haute Cour de justice irlandaise) demande alors l'avis de la CJUE pour statuer sur cette affaire.

## Quelles sont les motivations de la CJUE ?

La CJUE a désigné, Yves Bot, avocat général, pour instruire cette affaire. Par décision du Conseil européen, la CJUE dispose aujourd'hui de 11 avocats généraux et selon l'article 252 du Traité sur le fonctionnement de l'Union européenne :
« L'avocat général a pour rôle de présenter publiquement, en toute impartialité et en toute indépendance, des conclusions motivées sur les affaires qui, conformément au statut de la Cour de justice de l'Union européenne, requièrent son intervention. »

Dans ses conclusions, rendues publiques le 23 septembre 2015, Yves Bot étudie plusieurs questions fondamentales auxquelles il apporte les réponses suivantes :

- Quel est le rôle et quelles sont les capacités d'une autorité de régulation nationale face aux accords européens comme le *Safe Harbor* ? Peut-elle enquêter et agir contre des entreprises couvertes par ce type d'accord ?

*Une autorité nationale de protection des données a le droit et le devoir de défendre*

*les citoyens même en présence d'un accord européen*

- Que se passe-t-il lorsqu'un accord passé il y a 15 ans (le *Safe Harbor* est en vigueur depuis 2000) n'est pas révisé alors qu'il a été porté à la connaissance du public que des traitements de données personnelles ont été effectués en dehors des finalités prévues par cet accord ?

*La Commission européenne devait vérifier périodiquement la conformité du Safe Harbor aux standards de protection des données européens*

- Peut-on considérer que l'accès aux données des européens par les services de renseignement américains respecte les principes de proportionnalité et de finalités explicites qui sont jugés nécessaires au respect des droits fondamentaux en Europe, y compris lorsque sont invoqués les motifs de sécurité nationale ?

*Les conditions de respect des principes de proportionnalité et de finalités explicites ne sont pas respectés par les services de renseignement américains*

- Comment faire respecter les droits des citoyens européens lorsqu'il n'existe pas de possibilité de recours juridictionnel respectant les standards européens dans le pays qui reçoivent leurs données personnelles ?

Les citoyens européens ne disposent pas des garanties nécessaires à l'exercice de leurs droits contre le traitement de leurs données par les services de renseignement

- La Commission européenne aurait-elle dû d'elle-même suspendre le transfert des données personnelles ou au moins réviser périodiquement le *Safe Harbor* afin de vérifier que les critères de conformité prévus à l'origine continuaient d'être respectés ?

*Oui en conséquence, le Safe Harbor doit être invalidé et suspendu*

Les conclusions de l'avocat général de la CJUE étant consultatives, il faudra attendre le 6 octobre 2015 pour que la CJUE rende son jugement définitif en déclarant invalide la décision 2000/520 de la Commission du 26 juillet 2000 instaurant le principe de « Safe Harbor ».

Dans son communiqué de Presse , La CJUE indique :

« *Pour toutes ces raisons, la Cour déclare la décision de la Commission du 26 juillet 2000 invalide. Cet arrêt a pour conséquence que l'autorité irlandaise de*

*contrôle est tenue d'examiner la plainte de M. Schrems avec toute la diligence requise et qu'il lui appartient, au terme de son enquête, de décider s'il convient, en vertu de la directive, de suspendre le transfert des données des abonnés européens de Facebook vers les États-Unis au motif que ce pays n'offre pas un niveau de protection adéquat des données personnelles.* »

## Que va-t-il se passer maintenant ?

Tout d'abord, l'autorité de contrôle irlandaise va devoir mener des investigations et prendre une décision concernant l'affaire Schrems/Facebook. Mais au-delà de cette affaire, il s'ouvre une période d'incertitude juridique pour tous les acteurs (fournisseurs américains et client européens). Des clarifications rapides sont attendues de la part de la commission européenne mais également du groupe de travail des CNIL européennes (G29). Dans ce contexte, il est fort probable qu'un Safe Harbor v2 voit le jour rapidement pour prendre en compte les exigences européennes.

Dans l'immédiat, il est fortement recommandé aux entreprises de procéder à un audit afin de répertorier tous les traitements de données personnelles dont le transfert s'est appuyé sur la base juridique du Safe Harbor. Notons pour finir qu'il existe d'autres possibilités pour transférer légalement des données personnelles vers les états-unis : les Binding Corporate Rules (BCR), les clauses contractuelles types (CCT) ou encore, lorsque c'est possible, les exceptions à l'interdiction des flux transfrontières visées à l'article 69 de la loi Informatique et libertés.