Forum ATENA

... à la convergence du numérique, des entreprises et de l'enseignement supérieur

Le Cloud Souverain

Mythe ou réalité

Forum Atena – 25 Avril 2013

Olivier Iteanu, Avocat

&

Didier Soucheyre, Fondateur et Président de Neo Telecoms

ITEANU
Société d'Avocats | Law Office

Neo Telecoms

Google Apps dans les grandes entreprises : Valeo “sort du placard” !

Discrétion ? Précaution ? Peu importe la raison de ce long silence ; Valeo vient de publier un communiqué officiel qui confirme une information que beaucoup d’entre nous connaissions depuis longtemps, mais ne pouvions pas divulguer :

Valeo aura, fin 2009, migré l’intégralité de ses 30 000 utilisateurs de postes de travail sur Google Apps Premier Edition.

- Oui, mais est-ce une bonne idée ?
  - La CNIL relève ainsi que « l’autorité norvégienne a interdit l’utilisation de Google Docs (…) lorsque des données à caractère personnel sont concernées. »

Difficile de ne pas travailler avec eux…

- Etc…

Le buzz, pourquoi ?

- Juin 2011, déclaration de Gordon Frazer, Directeur Général de Microsoft UK, à l'occasion du lancement de Office 365 « *Msft, en tant que Société dont le siège social est aux Us, doit se conformer aux lois locales, dont la loi us* » et il ajoute que Msft se considère tenu par le Patriot Act même pour les données hébergées dans des Datacenters de l'Ue
- Août 2011, interview d'un représentant Google par le magazine Allemand WirtschaftsWoche, qui admet que Google se soumet au Patriot Act quand il reçoit des demandes des autorités us sur des utilisateurs qui ont des données hébergées dans l'Ue.

Historique du « Patriot Act »

- Loi passée le 26 Oct. 2001, en réaction aux attaques terroristes du 11 Sept.
  - « USA PATRIOT » est un acronyme :
    - **U**niting (and) **S**trengthening **A**merica (by) **P**roviding **A**ppropriate **T**ools **R**equired (to) **I**ntercept (and) **O**bstruct **T**errorism
- De nombreuses dispositions prises pour renforcer les pouvoirs de contrôle et d'investigation
- Création de fonds de financement des activités anti-terroristes, *procédures de surveillance*, dispositions anti-blanchiment, sécurité des frontières, nouveaux pouvoirs au FBI, indemnisation des familles de victimes, etc.

Des dispositions sensibles

- établies pour être temporaires...
  - La plupart des dispositions sensibles prises en urgence au lendemain des événements avaient vocation à être temporaires, et ne durer que jusqu'au 31 Déc. 2005
- … mais qui durent
  - L'application de ces dispositions a été étendue en Mars 2006, puis le 26 Mai 2011 pour trois de ses dispositions clef modifiant le Foreign Intelligence Surveillance Act de 1978 (FISA)
    - Écoutes itinérantes (§206 du Patriot Act « roving surveillance »)
    - Surveillance d'individus étrangers (§207 du Patriot Act « lone wolf terrorists »)
    - **Dispositions facilitant l'accès à des documents commerciaux** (§215 du Patriot Act « library records »)
    - Accès aux données de connexion (§210), écoutes électroniques (§212), avec des pouvoirs étendus des autorités administratives et un contrôle judiciaire très limité, etc.

Dispositions facilitant l'accès à des documents commerciaux (1)

- **Dispositions facilitant l'accès à des documents commerciaux** (§215 du Patriot Act « library records »)
  - *Dénommée ainsi par ses opposants, suite à une demande d'amendement formée par la American Library Association, qui affirmait que la généralité de ses termes permettrait, par exemple, au gouvernement US d'accéder secrètement aux données relatives à l'usage des bibliothèques américaines par toute personne simplement suspectée de terrorisme*

- **Permet au directeur du FBI de solliciter d'un juge l'autorisation de demander la production de :**
  - « any tangible things (including books, records, papers, documents, and other items »
    - Définition très large : tous types de documents
  - Concernant toute personne étrangère, ou tout citoyen américain
    - sauf si ce dernier exerce une activité protégée par le 1er amendement de la constitution des USA (donc une activité liée à l'exercice de la liberté de religion et d'expression, la liberté de la presse ou le droit à s'« assembler pacifiquement »)
      - Champs d'action très large même pour les personnes ou entités US
      - Champ illimité pour les personnes ou entités non américaines

Dispositions facilitant l'accès à des documents commerciaux (2)

- Permet au directeur du FBI de solliciter d'un juge l'autorisation de demander la production (suite) :
  - Dans le cadre d'une enquête relative à des activités de terrorisme international, ou des activités d'espionnage clandestines
    - Il faut convaincre le juge d'activités suspectées de ce type
  - L'autorisation délivrée ne divulgue pas l'objet de l'enquête, et s'impose à tout détenteur des informations recherchées
  - Il est interdit au détenteur des informations de divulguer à quiconque qu'il a été sollicité par le FBI
    - Caractère « secret » de la sollicitation et de sa motivation
- Le détenteur des informations est légalement protégé par la loi américaine et n'est pas responsable à l'égard des tiers des conséquences de cette divulgation
    - Pas de recours aux US contre la personne divulguant ces informations au FBI, quelles que soient ses obligations envers la personne qui les lui a confiées

Prestataires « Cloud »

- Un prestataire de service « Cloud » relevant de la juridiction américaine est susceptible de faire l'objet de ce type de demandes
  - Dans le cadre d'une enquête dirigée contre une personne ou une entité française, par exemple, suspectée d'activités terroristes ou d'espionnage
- Le prestataire de service « Cloud »
  - a l'obligation de fournir les informations en sa possession
  - a l'interdiction d'en informer son client
  - ne peut être responsable de cette divulgation selon la loi américaine
    - Y compris si cette divulgation la conduit à violer, par exemple, ses engagements contractuels de confidentialité ou de sécurité des données, ou les engagements qu'elle aurait pris de respecter les principes du Safe Harbor sur la base desquels une entité française se reposerait pour permettre le transfert de données personnelles en dehors du territoire de l'Union Européenne

Comment se prémunir ?

- Passer contrat avec des entités non-américaines
  - Quid des Sociétés européennes filiales de groupes US – exemple : Microsoft, Google, Amazon,...
  - Les éviter ?
    - Sinon : éviter les Sociétés directement contrôlées par des Sociétés US, en faire une clause *intuitus personnae*
- Soumettre le contrat passé avec la filiale à la loi française et à la juridiction des tribunaux français, rendre responsable le prestataire des divulgations opérées en infraction avec les dispositions contractuelles
  - Interdire au prestataire de Cloud la sous-traitance, notamment à des entités américaines ou basées aux US
    - Voire même, interdire au prestataire de Cloud que les personnels en charge de l'exécution du contrat (et ceux des sous-traitants autorisés) soient des citoyens de nationalité américaine
- **Circonscrire géographiquement la localisation des données : <u>Réelle</u> préoccupation légale par ailleurs en raison de l'interdiction *a priori* d'exportation des données personnelles en dehors de l'Union Européenne (Cloud souverain ?)**

En France aussi …

Interceptions (ex écoutes)

- En cas de flagrance, le juge des libertés les autorise (art. 74-2 du CPP)
- Si peine encourue est égale ou supérieure à 2 ans de prison, le juge d'instruction les autorise (art. 100 du CPP)
- Les interceptions de sécurité hors contrôle d'un juge autorisées par le 1er Ministre (Loi 10/07/1991)

Captations

- Le juge d'instruction l'autorise *« en tous lieux »* et les données sont placées sous scellés (Loppsi2 du 14/03/11 création d'une Section 6bis du CCP *« De la captation des données informatiques »*)
- Pouvoir plus général du juge d'instructions de perquisition (Art. 97 et svts du CPP)

En conclusion

- La Patriot Act est une réalité en marche
  - Dont on ne connaît pas l'ampleur, ni les modalités (durée de conservation, qui a accès aux données captées …)
- Les entreprises françaises et leurs données peuvent être concernées
  - Si elles ont recours à « un prestataire US »
    - Le contrat ne pourra pas grand chose
- Au minimum, il faut donc gérer ce risque juridique réel en fonction de la criticité des données confiées