Le USA Patriot Act : risque majeur pour la confidentialitÃ© des donnÃ©es dans le Cloud
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 12/3/2012 13:30:00

Avec le dÃ©veloppement rapide du SaaS (Software As A Service) les entreprises se posent lÃ©gitimement la question de la sÃ©curitÃ© de leurs donnÃ©es dans le Cloud. Si le problÃ¨me est souvent examinÃ© en termes technique de sÃ©curitÃ© physique des donnÃ©es, il doit aussi lâ□□Ãªtre en matiÃ¨re de sÃ©curitÃ© juridique de donnÃ©es parfois trÃ¨s sensibles.

Alain WEBER (Avocat Henri Leclerc & AssociÃ©s â□□ Membre du Conseil de lâ□□Ordre), **Marie CHAUMARD** (Avocat Henri Leclerc & AssociÃ©s) et **Jamal LABED** (Directeur GÃ©nÃ©ral & cofondateur dâ□□EasyVista) dressent les tenants et les aboutissants duÂ USA Patriot Act.

Compte-tenu de la prÃ©dominance des acteurs amÃ©ricains dans le domaine du SaaS, il convient donc de sâ□□interroger sur les risques que fait courir le Â« USA Patriot Act Â» auquel ils sont soumis, Ã la diffÃ©rence des Ã©diteurs europÃ©ens.

Ce document rÃ©digÃ© avec un avocat expert en matiÃ¨re de protection des donnÃ©es a pour objectif de faire un point dÃ©taillÃ© et argumentÃ© sur cette question centrale.

La lÃ©gislation rÃ©sultant de la mise en oeuvre de **lâ□□USA PATRIOT ACT** (Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism act) du 26 octobre 2001 prolongÃ©e jusquâ□□en juin 2015 impose aux entreprises de droit amÃ©ricain, ainsi quâ□□Ã leurs filiales dans le monde, et aux serveurs hÃ©bergÃ©s sur le territoire des Etats-Unis quelque soit la nationalitÃ© des entreprises qui les exploitent, ainsi qu'aux donnÃ©es hÃ©bergÃ©es en Europe par des sociÃ©tÃ©s de droit amÃ©ricain, des obligations permettant aux services de sÃ©curitÃ© amÃ©ricains dâ□□accÃ©der Ã des donnÃ©es Ã caractÃ¨re personnel.

1) Rappelons qu'une donnÃ©e personnelle est:

Â« (..) toute information relative Ã une personne physique identifiÃ©e ou qui peut Ãªtre identifiÃ©e, directement ou indirectement, par rÃ©fÃ©rence Ã un numÃ©ro dâidentification ou Ã un ou plusieurs Ã©lÃ©ments qui lui sont propres. Pour dÃ©terminer si une personne est identifiable, il convient de considÃ©rer lâensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accÃ¨s le responsable du traitement ou toute autre personne.

Constitue un traitement de donnÃ©es Ã caractÃ¨re personnel toute opÃ©ration ou tout ensemble dâopÃ©rations portant sur de telles donnÃ©es, quel que soit le procÃ©dÃ© utilisÃ©, et notamment la collecte, lâenregistrement, lâorganisation, la conservation, lâadaptation ou la modification, lâextraction, la consultation, lâutilisation, la communication par transmission, diffusion ou toute autre forme de mise Ã disposition, le rapprochement ou lâinterconnexion, ainsi que le verrouillage, lâeffacement ou la destruction.

Constitue un fichier de donnÃ©es Ã caractÃ¨re personnel tout ensemble structurÃ© et stable de donnÃ©es Ã caractÃ¨re personnel accessibles selon des critÃ¨res dÃ©terminÃ©s. La personne concernÃ©e par un traitement de donnÃ©es Ã caractÃ¨re personnel est celle Ã laquelle se rapportent les donnÃ©es qui font lâobjet du traitement. Â».

Les donnÃ©es que vous hÃ©bergez sont donc concernÃ©es.

2) Plus prÃ©cisÃ©ment, la section 215 de ***lâUSA PATRIOT ACT*** et les sections 504, 505 et 358 autorisent des perquisitions soit sous le contrÃ´le dâun Juge soit hors contrÃ´le dâun Juge.

Ces actions peuvent demeurer secrÃ¨tes pendant une durÃ©e indÃ©terminÃ©e.

3) Il en rÃ©sulte que la personne concernÃ©e ignore les donnÃ©es ayant Ã©tÃ© consultÃ©es ou saisies du fait des perquisitions, ainsi que lâusage qui en est fait ou qui en sera fait; elle ignore Ã©galement les modalitÃ©s de conservation, ainsi que les services de renseignement ou de police qui en ont Ã©tÃ© rendus destinataires.

4) Lâ Union EuropÃ©enne a Ã©dictÃ© des textes protecteurs des donnÃ©es personnelles.

La Directive 95/46 CE du Parlement EuropÃ©en et du Conseil du 24 octobre 1995 rappelle les principes selon lesquels les systÃ¨mes de traitement de donnÃ©es sont au service de lâHomme et quâils doivent - quelle que soit la nationalitÃ© ou la rÃ©sidence des personnes physiques - respecter les libertÃ©s et droits fondamentaux de ces personnes, notamment la vie privÃ©e.

5) Le dispositif particulier dit de Â« Safe Harbour Â» ou Â« SphÃ¨re de sÃ©curitÃ© Â» a Ã©tÃ© mis en place concernant les garanties apportÃ©es en cas de flux de donnÃ©es entre des entreprises amÃ©ricaines et des entreprises europÃ©ennes.

6) Le systÃ¨me repose sur lâauto-certification des entreprises amÃ©ricaines qui dÃ©clarent adhÃ©rer Ã une sÃ©rie de principes de protection de donnÃ©es personnelles et de protection de la vie privÃ©e.

7) Ces principes basÃ©s sur ceux de la Directive 95/46 du 26 octobre 1995 ont Ã©tÃ© nÃ©gociÃ©s entre les autoritÃ©s amÃ©ricaines et la Commission EuropÃ©enne; ils sont publiÃ©s par le MinistÃ¨re du Commerce des Etats-Unis.

8) La Commission EuropÃ©enne a adoptÃ© le 26 juillet 2000 une dÃ©cision dâ□□adÃ©quation qui reconnaÃ®t que les principes de Â« Safe Harbour Â» assurent une protection adÃ©quate pour les besoins des transferts de donnÃ©es Ã caractÃ¨re personnel depuis lâ□□Union EuropÃ©enne.

9) Cependant, la dÃ©cision dâ□□adÃ©quation de la Commission EuropÃ©enne en date du 26 juillet 2000 est antÃ©rieure Ã la promulgation de la lÃ©gislation rÃ©sultant de lâ□□USA PATRIOT ACT du 26 octobre 2001.

10) Le secret entourant les activitÃ©s des services de renseignement relevant du Gouvernement des Etats-Unis empÃªche toute vÃ©rification du respect des principes de la Directive notamment sur les activitÃ©s de recueil, de traitement, de conservation des donnÃ©es et empÃªche tout contrÃ´le des intÃ©ressÃ©s sur ces activitÃ©s.

11) Il en rÃ©sulte lâ□□ineffectivitÃ© du Â« Safe Harbour Â» pour garantir la confidentialitÃ© des donnÃ©es hÃ©bergÃ©es auprÃ¨s de sociÃ©tÃ©s de droit amÃ©ricain ou de leurs filiales, ou dans des serveurs situÃ©s aux Etats-Unis, notamment sur des plateformes cloud.

12) Dans le but de pallier lâ□□ineffectivitÃ© de Â« Safe Harbour Â», lâ□□Union EuropÃ©enne a proposÃ© que, dans le cours du 1er semestre 2012, un rÃ¨glement intitulÃ© Â« General Data Protection Regulation Â» ainsi quâ□□une Directive intitulÃ©e Â« Police and Criminal Justice Data Production Directive Â» soient publiÃ©s.

13) Ces instruments prÃ©voient dans ce domaine lâ□□accroissement des garanties qui devront Ãªtre offertes par les pays tiers destinataires de donnÃ©es, et notamment la prise en compte par la Commission, afin dâ□□Ã©mettre des dÃ©cisions dâ□□adÃ©quation comme cela a Ã©tÃ© le cas pour Â« Safe Harbour Â», de la lÃ©gislation relative Ã la sÃ©curitÃ© publique, la dÃ©fense, la sÃ©curitÃ© nationale et la criminalitÃ©, ainsi que lâ□□existence et lâ□□activitÃ© effective dans le pays tiers dâ□□une autoritÃ© indÃ©pendante de protection des donnÃ©es Ã caractÃ¨re personnel en charge de ce domaine et coopÃ©rant avec les autoritÃ©s de lâ□□Union.

En lâ□□Ã©tat, il est manifeste que les dispositions du USA PATRIOT ACT ci-avant relevÃ©es, Ã savoir notamment les sections 215, 504, 505 et 358, sont incompatibles avec les exigences de protection et de confidentialitÃ© de lâ□□Union EuropÃ©enne.

Il convient Ã©galement de considÃ©rer que la dÃ©cision dâ□□adÃ©quation de la Commission sur laquelle sâ□□appuie le dispositif de Â« Safe Harbour Â» est caduque, du fait de la mise en oeuvre de la lÃ©gislation dÃ©rogatoire rÃ©sultant du USA PATRIOT ACT.

En effet, cette lÃ©gislation met Ã nÃ©ant tous les principes de protection de la confidentialitÃ© des donnÃ©es, tels que ces principes sont Ã©dictÃ©s par la lÃ©gislation europÃ©enne, rendant ainsi ineffective la confidentialitÃ© prÃ©tendument attachÃ©e aux traitements de donnÃ©es rÃ©alisÃ©s dans le cadre du dispositif de Â« Safe Harbour Â» notamment pour les donnÃ©es hÃ©bergÃ©es sur plateforme Cloud.

En revanche, il semble que le USA PATRIOT ACT est impuissant pour contraindre une sociÃ©tÃ© EuropÃ©enne â□□ mÃªme si cette derniÃ¨re a une filiale aux Etats Unis â□□ Ã communiquer ou laisser accÃ©der les autoritÃ©s amÃ©ricaines aux donnÃ©es personnelles qu'elle hÃ©berge en Europe ou dans un autre pays Ã l'extÃ©rieur des USA.

Mais la filiale situÃ©e aux USA est soumise au USA PATRIOT ACT pour les donnÃ©es qu'elle hÃ©berge.

En d'autres termes, la prÃ©sence aux USA d'une filiale d'une sociÃ©tÃ© EuropÃ©enne, ne permet pas d'atteindre la mÃ¨re ou la soeur de ladite filiale, ni les donnÃ©es qu'elles hÃ©bergent en dehors des USA