01netPro.

14/12/2012 19:43

Benard Lamon

Cloud : assez de la tarte à la crème du Patriot Act !!! par @Bernard_Lamon

Cloud : assez de la tarte à la crème du Patriot Act !

Avant de s'inquiéter du Patriot Act américain, les entreprises devraient s'intéresser à d'autres risques liés au cloud, plus concrets et plus probables. Parmi ceux-ci : l'e-discovery, le piratage de données par les salariés et des contrats illisibles.

Chaque discussion sur l'intérêt de passer au cloud est marquée par un passage obligé : *« Attention, il y a le Patriot Act. »* Derrière cette courte phrase, se cache une peur, exploitée parfois à des fins marketing. Le discours, souvent implicite, est clair : si vous confiez vos données d'entreprise à un prestataire extérieur, un concurrent américain peut y avoir accès et vous les « siphonner ».

En France, le Patriot Act s'appelle Lopssi

Pour éclaircir le propos, je ne travaille pas pour le compte d'un cabinet de lobbying, et j'aime les Etats-Unis et les autres pays anglo-saxons. Comme je les aime bien, je connais aussi leurs qualités, dont celle de souhaiter imposer leurs intérêts et leur mode de pensée. L'autre intérêt de parler anglais et d'être opérationnel (un peu…) en droit américain est de pouvoir vous dire une chose simple : le Patriot Act existe aussi en France… comme dans tous les pays démocratiques du monde.

Dans la foulée des attentats du 11septembre 2001, un arsenal législatif a été adopté dans beaucoup de pays. Ces lois permettent à la police et aux services de renseignements d'avoir accès, sur autorisation d'un juge, à des données détenues par ou sur une personne soupçonnée d'être liée à une entreprise terroriste.

L'équivalent français du Patriot Act s'est d'abord appelé Lopssi (Loi d'orientation et de programmation pour la performance de la sécurité intérieure) puis Lopssi 2. On rappellera que la lutte contre le terrorisme est confiée en France à la DCRI (Direction centrale du renseignement intérieur, fusion des anciens Renseignements généraux et de la DST), qui est un service de police judiciaire.

Ce qui signifie concrètement que notre cabinet demande (et obtient) deux ou trois fois par mois des données d'entreprise dans des conditions similaires à celles du Patriot Act. Par exemple, des juges nous fournissent des informations fournies par les fournisseurs d'accès à internet pour identifier des internautes, ou des données liées à des saisies (de contrefaçon ou de concurrence déloyale). Nous avons une volée de dossiers dans lesquels des policiers (dont ceux de la DCRI) ont utilisé les lois en vigueur pour récupérer des données d'entreprise…

Par ailleurs, la portée exacte du Patriot Act est à relativiser. Plusieurs décisions de jurisprudence en ont limité les impacts.

Les trois principaux risques du cloud

Mais le pire n'est même pas là. Le pire est qu'à force de se fixer sur cette tarte à la crème du Patriot Act, on ne voit pas les vraies questions soulevées par le cloud, dans la vraie vie des entreprises. Les dangers au quotidien sont bien plus importants que ceux

Cloud : assez de la tarte à la crème du Patriot Act !!! par @Bernard_Lamon

causés par l'application de cette loi antiterroriste américaine. Heureusement, il existe des solutions.

En pratique, il faut distinguer trois risques principaux à gérer au moment de souscrire à une offre cloud.

Le risque interne : le cloud fait sortir les données des locaux de l'entreprise. Rien ne garantit qu'un salarié (stagiaire, prestataire, dirigeant…) ne « siphonne » ces informations. Car le cloud s'accommode très bien, et va même de pair, avec le BYOD (Bring Your Own Device). La solution ? Pour résoudre 80 % du risque avec 20 % d'efforts, il suffit d'écrire une charte informatique en se donnant les moyens d'aboutir à un document de qualité. Eviter les copier-coller sur internet. Et faites se rencontrer juriste, DSI et DRH… Dans la réalité, rares sont les entreprises à avoir une telle charte. Quant à celles qui existent… leur qualité est très variable (pour rester charitable).

Le risque relatif au prestataire de service cloud. Quand on confie ses données à un tiers, il paraît évident de se préoccuper d'abord des relations qu'on entretient avec lui… avant de se demander si une autorité judiciaire risque d'exiger qu'on lui remette telle ou telle information. Donc, il faut examiner le contrat avec ce tiers. Pour l'analyser, on tentera d'atteindre trois ou quatre objectifs simples. L'idéal est d'abord d'obtenir un contrat lisible, autrement dit qui peut être plaidé s'il n'est pas respecté. Ensuite, un contrat soumis à une loi d'un pays que vous ne maîtrisez pas, et devant un juge inaccessible, n'est pas un contrat : c'est un recueil de bonnes intentions. En d'autres termes : les promesses n'engagent que ceux qui y croient. Et si vos données sont inaccessibles pendant quarante-huit heures ou perdues, ne venez pas vous plaindre.

Le risque lié à l'e-discovery. Si on parle du droit américain, plutôt que du Patriot Act, préoccupez-vous de la procédure de l'e-discovery. Cela peut vous coûter beaucoup plus cher, et c'est beaucoup plus fréquent. Faire du business aux Etats-Unis a un coût, comme faire du business partout dans le monde (locaux, salariés, marketing, risque juridique…). Le risque juridique est souvent négligé par le dirigeant français (hélas ! dit l'avocat, en essuyant une larme). Or, il coûte potentiellement beaucoup plus cher aux Etats-Unis qu'en France, même s'il existe dans les deux pays. Le travail du chef d'entreprise ou du cadre dirigeant, c'est justement de gérer ce risque… pour pouvoir prendre des risques.

Conclusion optimiste : le cloud est un vivier d'opportunités (économies, agilité des process…), mais le monde environnant n'est pas celui des Bisounours, et avec quelques précautions, on limitera sérieusement (mais jamais totalement) les risques.

Bernard Lamon

Bernard Lamon anime la société d'avocats Lamon & Associés, qui traite exclusivement des questions relatives au droit de l'informatique, de la communication de l'innovation de la concurrence déloyale. La société intervient en conseil et en contentieux, convaincue que chacune de ces activités enrichit l'autre par l'expérience qu'elle confère. L'équipe a également une forte activité de formation (INPI France, école des avocats, entreprises…).