EDI
Pays : France
Périodicité : Mensuel
OJD : 11617

Date : FEV 17
Page de l'article : p.76,78,80
Journaliste : Pierre-Antoine Merlin

Dossier | Cloud | *Protection des données*

Par Pierre-Antoine Merlin

OPPORTUNITÉS DANS LA GARANTIE DES DONNÉES

Les craintes associées à la cybercriminalité, mais aussi à ses conséquences sur la chaîne de valeur, doivent être dépassées. État des lieux et pistes de réflexion pour transformer une contrainte majeure en business lucratif.

Jamais le sujet de la protection des données dans le cloud n'a été aussi brûlant. Sur le plan économique et social, d'abord. La montée des périls, l'invasion du cyberterrorisme, les aléas juridiques, et jusqu'à cette inquiétude sourde qui étreint cœurs et esprits, tout concourt à créer dans l'opinion une boule de tension. Il faut encore y ajouter les enjeux législatifs et réglementaires, toujours plus nombreux chaque année. Ces évolutions, disparates dans leurs causes, mais convergentes dans leurs effets, seront-elles favorables au channel ? Tout porte à le croire. Au niveau des États comme à celui des acteurs de l'économie numérique, la prise de conscience se fait impérieuse. Tant il est vrai que la meilleure défense, c'est l'attaque.

Le cadre juridique en pleine transformation

Impossible, dans le cadre de cette enquête, de revenir en détail sur le match Europe-États-Unis dans la protection des données personnelles *(lire p. 72)*. C'est une saga aux multiples rebondissements, réactivée en permanence sous la pression politique, technique et commerciale. Aujourd'hui, le champ de bataille se présente non comme une série de tranchées aboutissant à la guerre de position, mais comme un écheveau de poupées russes. D'une part, la France est dotée de sa propre législation depuis 1978. D'autre part, elle doit transposer en droit français, sans relâche sous peine d'astreinte, les directives émanant de la Commission européenne. À l'arrivée, tout est contrecarré par les pratiques américaines, plus soucieuses de business que de protection de la vie privée, fût-elle dans le cloud. D'où les tentatives de compromis, plus ou moins durables, qui portent les doux noms de Privacy Shield et de Safe Harbor. Des dénominations bien pompeuses pour de petits arrangements entre amis d'un jour,

LES EXIGENCES DU SECNUMCLOUD QUI QUALIFIENT LES PRESTATAIRES

L'Agence nationale de la sécurité des systèmes d'information (Anssi) qui constitue le bras séculier des pouvoirs publics en termes de sécurité du cloud – et de tout ce qui s'y trouve – a beaucoup travaillé, ces derniers mois, pour publier dans les meilleurs délais son fameux référentiel. Celui-ci couvre, d'une part, *« les services d'informatique en nuage »*, et, d'autre part, *« la qualification de prestataires proposant de tels services »*. L'Agence a procédé à une expérimentation extensive, d'une durée de deux ans, pour avancer sur l'ensemble du dispositif technique et juridique. Deux niveaux seront exigés des prestataires pour être conformes : Essentiel ou Avancé, actuellement en voie de finalisation. Ce dernier référentiel d'exigences reprend les caractéristiques de l'ancien Secure Cloud Plus. Sur le site de l'Anssi figurent déjà plusieurs prestataires cloud en cours de qualification, notamment Oodrive avec des solutions de partage de fichiers et de travail collaboratif, et Orange Business Services avec une solution de synchronisation et de partage de documents.

« La loi pour une République numérique est un dispositif sans doute inédit dans le monde »

Axelle Lemaire, secrétaire d'État chargée du Numérique et de l'Innovation

et qui n'ont d'ailleurs jamais fonctionné. D'où, aussi et surtout, l'émergence de deux textes fondateurs, l'un français, l'autre européen, qui vont tout changer. Car comme par un fait exprès, ces deux initiatives vont dans le même sens. Côté français, la loi pour une République numérique, adoptée l'automne dernier par le parlement, fait obligation aux responsables du traitement des données personnelles d'informer les personnes physiques et morales sur la durée légale de conservation des informations. Autre innovation, les responsables du traitement sont tenus d'effacer les données privées émanant d'une personne mineure lors de leur collecte. *« C'est un dispositif inédit et expérimental en France, et sans doute dans le monde, à un tel niveau »*, a tenu à préciser Axelle Lemaire, secrétaire d'État chargée du Numérique et de l'Innovation. Côté européen, les choses avancent bien. Les démarches engagées reprennent grosso modo les textes français – à moins que ce soit le contraire. Ainsi le futur RGPD (Règlement général sur la protection des données) fait état des mesures précises et détaillées visant à décourager, financièrement et même pénalement, les éventuels fraudeurs. À partir de maintenant, toute organisation, publique ou privée, qui collecte, utilise ou partage des informations relatives aux citoyens européens devra se conformer aux nouvelles règles. Faute de quoi, elle risquera une amende allant jusqu'à 4 % de son C. A. Est-ce réaliste ? Selon un proche du dossier, *« c'est trop ou trop peu. Pour les Gafa, il y aura toujours moyen de s'arranger en envoyant à Bruxelles une batterie de lobbyistes et d'avocats. À l'autre bout du spectre, dans le cas d'un petit éditeur par exemple la sanction sera trop lourde, donc inapplicable »*.

Une manne pour la chaîne de valeur

Cependant, certains éditeurs ont la chance de s'être lancés, dès les débuts de l'informatique à la demande, dans la protection de l'utilisateur. Pour ceux qui, de surcroît, ont misé sur le channel pour populariser leurs solutions, le choix s'est révélé judicieux. *« Être conforme à la politique de la Cnil, préparer les utilisateurs au futur règlement européen, c'est justement notre métier de base »*, explique Marine Marçais, Partner Account Manager chez Acronis. Même constat pour Sylvie Le Roy, Network Director, EMEA de l'organisme de certification Uptime Institute, l'un des plus réputés du secteur au plan international. *« Les sociétés commencent à se préoccuper de ce qui va se passer à Bruxelles. C'est pour cela que nous prenons les devants. Pour nous, c'est beaucoup d'activité en perspective vis-à-vis de nos partenaires et clients. Un peu comme pour le Brexit. »* D'autres fournisseurs, comme Eset, ont trouvé la parade pour assurer aux utilisateurs la sécurité des informations stockées dans le cloud. *« Nous proposons des solutions de chiffrement, ainsi que*

LE CODE DE CONDUITE PORTÉ PAR LES HÉBERGEURS

Il manquait une initiative forte pour promouvoir le métier d'hébergeur, spécialement dans le domaine de la protection des données. Plusieurs acteurs ont fait cause commune pour agir dans l'intérêt des acteurs de la chaîne. Parmi eux, on trouve le français Outscale, seul rescapé de l'aventure du cloud souverain, spécialisé depuis le début dans le IaaS.

La voix des fournisseurs portée par le Cloud Infrastructure Services Providers in Europe (Cispe),

Autre participant, le groupe Ikoula. Lui, n'était pas embarqué dans le cloud souverain mais a toujours œuvré dans et pour le cloud français. C'est pour développer ce dernier, que Jules-Henri Gavetti *(photo)* s'investit dans le Cispe. *« Le développement du marché du cloud et de l'hébergement est, intrinsèquement, lié à la confiance accordée par les clients,* estime-t-il. *Sans une présence au niveau juridique, permettant de mieux adapter les législations et d'éviter les incertitudes, le marché ne peut ni se développer, ni se pérenniser. »* Plusieurs dizaines d'hébergeurs ont rejoint le Cispe, qui souhaite ainsi *« définir le rôle et les responsabilités des fournisseurs d'infrastructures dans le traitement des données hébergées, ainsi que mettre en place de règles communes au niveau européen »*. Une démarche opportune au moment où le Règlement général sur la protection des données s'apprête à clore le débat.

« Définir le rôle et les responsabilités des fournisseurs [...] et mettre en place des règles communes au niveau européen »

Jules-Henri Gavetti, CEO et cofondateur d'Ikoula

« Renforcer l'écosystème du logiciel et des éditeurs par la SaaS Academy »

Alban Schmutz, ancien président de la SaaS Academy et vice-président d'OVH

de l'authentification forte, explique Benoît Grunemwald, directeur des opérations de la filiale française. *En effet, en dehors du moment où la donnée est utilisée et donc déchiffrée, sa protection est assurée contre les accès non autorisés par son chiffrement. L'authentification forte garantit que la personne qui se connecte au cloud est bien celle qu'elle prétend être. On augmente aussi la perception que chaque utilisateur possède de sa propre responsabilité vis-à-vis des données.* » Responsabilité : le mot est lancé. Mais elle ne se conçoit pas sans la confiance. Celle-ci est essentielle pour garantir une sorte de protectionnisme virtuel dans un océan de libre-échange.

Confiance et certification

Le cloud étant, par nature, nébuleux, ses promoteurs éprouvent régulièrement le besoin de faire cause commune pour accompagner l'ensemble des protagonistes. C'est tout le sens de la SaaS Academy, lancée il y a deux ans à l'initiative des pouvoirs publics et de grands acteurs de la chaîne de valeur. Alban Schmutz, vice-président d'OVH et ancien président de cette structure, a ainsi planté le décor : il s'agit *« de renforcer l'écosystème du logiciel, mais aussi tout éditeur désireux d'être accompagné par ce programme. Compter des éditeurs plus forts pour leur développement en France ou à l'export, avec des modèles économiques adaptés aux enjeux du cloud, des équipes techniques prêtes à y répondre avec les financements associés, telles sont les solutions que nous essaierons d'apporter. »* Se sont vite associés à cette démarche, de grands noms parmi lesquels Intel, IBM, Microsoft, VMware et Crayon. Et cette liste est loin d'être close. Autre initiative : le label Cloud Confidence. Créé voilà deux ans, il s'efforce de crédibiliser et de normaliser l'univers du cloud pour que chacun y trouve son compte, y compris en s'adjoignant les services d'un cabinet d'audit. L'idée est de présenter au public une certification objective, reconnue par la communauté des acteurs comme une caution scientifique. Mais c'est sans doute le référentiel Anssi sur les clouds de confiance, SecNumCloud, qui fait le plus autorité. Pour au moins deux raisons. D'abord, l'Agence nationale de la sécurité des systèmes d'information est l'organisme officiel de l'État français pour la sécurisation du cloud. Ensuite, non seulement elle détermine avec un grand degré de précision ce que doit être « l'informatique en nuage », mais encore elle codifie la qualification des prestataires de cloud. Elle guide les intervenants français perdus dans un nuage transformé en brouillard *(lire l'encadré ci-dessous »).* ■

« On augmente la perception que chaque utilisateur possède de sa responsabilité vis-à-vis des données »

Benoît Grunemwald, directeur des opérations France, Eset

QUARANTE ANS DE CAFOUILLAGES JURIDIQUES

En application du rapport Nora-Minc, qui s'est saisi du problème au milieu des années 1970, la France se dote dès 1978 d'une loi tout à fait pionnière sur la protection des données personnelles. Dans le même mouvement, elle crée la Cnil (Commission nationale de l'informatique et des libertés). Cet embryon d'arbitre, impartial et régulateur, voulu par l'encore jeune Alain Minc pour organiser ce qu'il appelle « l'agora informationnelle », inspirera ce qui va suivre en Europe. Avec un bémol : à mesure que les États européens prennent des initiatives semblables à la Cnil, la Commission européenne gagne en influence. Pendant ce temps, fidèle à son habitude, la France traîne des pieds et prend du retard pour transposer dans son corpus juridique les directives et circulaires de Bruxelles. Il faut désormais plusieurs années pour adopter les textes. Un comble ! Outre-Atlantique, le problème est plus simple, puisqu'il ne se pose pas. En dépit des efforts consentis par le sous-secrétaire d'État David Aaron, figure de proue de l'ère Clinton et voyageur infatigable, le rapprochement entre grandes puissances ne se fait pas. Qu'importe ? Depuis longtemps, cette controverse a dépassé le cadre des États-nations. Elle incarne simplement le rapport de forces entre le Gafa et le reste du monde.