Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Quel cadre pour l’État d’urgence et la copie des données informatiques ?

Le gouvernement a entendu le Conseil constitutionnel, et fixé cette fois-ci un cadre très précis à la copie et l'utilisation des données informatiques saisies lors des perquisitions administratives réalisées dans le cadre de l'état d'urgence.

Ce mardi matin, nous expliquions que pour faire revenir la possibilité de saisir des données informatiques lors de perquisitions administratives organisées dans le cadre l'état d'urgence, le gouvernement aurait l'obligation de se conformer aux demandes d'encadrement fixées par le Conseil constitutionnel dans sa décision du 19 février 2016. Celui-ci avait en effet censuré le dispositif prévu à l'origine en novembre 2015, qui autorisait de copier les données accessibles sur place, sans aucun encadrement, ni sur la forme, ni sur le fond.

Nous avions ainsi résumé les préconisations des sages du Palais Royal :
• N'autoriser la copie que si une infraction est constatée lors de la perquisition administrative ;
• Limiter la copie aux données en lien avec l'infraction constatée ;
• Prévoir un cadre strict de conservation et d'exploitation des données saisies ;
• Faire entrer le juge dans la boucle.

Jean-Jacques Urvoas, ministre de la Justice, au Sénat.

Or il faut reconnaître au gouvernement, sans doute influencé en ce sens par le ministre de la justice Jean-Jacques Urvoas, d'avoir su prendre parfaitement acte des demandes du Conseil constitutionnel. Tel que présenté en conseil des ministres et tel qu'il devrait être adopté par le Parlement, le projet de loi prorogeant l'état d'urgence fixe un cadre très précis, même s'il ne va pas aussi loin dans le filtrage que ce qu'ont souhaité les membres du Conseil.

PAS D'ACCÈS AU CLOUD, CONSULTATION OBLIGATOIRE D'UN JUGE,…

Nous avons mis en gras les éléments les plus importants du projet de loi, qui concernent notamment l'obligation de motiver la copie des données et de ne les consulter qu'après l'aval d'un juge administratif qui aura 48 heures pour se prononcer. On notera au passage que la copie est désormais limitée aux seules « *données contenues dans tout système informatique présent sur les lieux de la perquisition* », ce qui doit exclure en principe l'accès aux données stockées dans le Cloud – auparavant celle-ci était prévue par une référence aux « *données accessibles à partir du système initial ou disponibles pour le système initial* », qui a disparu.

« *Si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée, les* ***données contenues dans tout système informatique ou équipement terminal présent sur les lieux*** *de la perquisition peuvent être saisies, soit par leur copie, soit par la saisie de leur support lorsque la copie ne peut être réalisée ou achevée pendant le temps de la perquisition.*

La copie des données ou la saisie des systèmes informatiques ou des équipements terminaux est réalisée en présence de l'officier de police judiciaire. L'agent sous la responsabilité duquel est conduite la perquisition rédige un procès-verbal de saisie qui ***en indique les motifs*** *et dresse l'inventaire des matériels saisis. Une copie de ce procès-verbal est remise aux personnes mentionnées au deuxième alinéa du présent I. Les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition.* ***À compter de la saisie, nul n'y a accès avant l'autorisation du juge****.*

L'autorité administrative ***demande au juge des référés du tribunal administratif d'autoriser en tout ou partie leur exploitation****. Au vu des éléments révélés par la perquisition et, s'il l'estime utile, des données et matériels saisis, il* ***statue dans un délai de quarante-huit heures*** *à compter de sa saisine sur la régularité de la saisie et la demande de l'autorité administrative.* ***Sont exclus de l'autorisation les éléments dépourvus de tout lien avec la menace*** *que constitue le comportement de la personne concernée pour la sécurité et l'ordre publics.* ***En cas de refus*** *du juge des référés, et sous réserve de l'appel mentionné au dixième alinéa,* ***les données copiées sont détruites*** *et les supports saisis sont restitués à leur propriétaire.*

Pendant le temps strictement nécessaire à leur exploitation autorisée par le juge des référés, les données et les supports saisis sont conservés sous la responsabilité du chef du service ayant procédé à la perquisition et à la saisie. Les systèmes informatiques ou équipements terminaux sont ***restitués à leur propriétaire****, le cas échéant après qu'il a été procédé à la copie des données qu'ils contiennent,* ***à l'issue d'un délai maximal de quinze jours*** *à compter de la date de leur saisie ou de celle à laquelle le juge des référés, saisi dans ce délai, a autorisé l'exploitation des données qu'ils contiennent.* ***À l'exception de celles qui caractérisent la menace que constitue pour la sécurité et l'ordre publics le comportement de la personne concernée****,* ***les données copiées sont détruites à l'expiration d'un délai maximal de trois mois*** *à compter de la date de la perquisition ou de celle à laquelle le juge des référés, saisi dans ce délai, en a autorisé l'exploitation.*

En cas de difficulté dans l'accès aux données contenues dans les supports saisis ou dans l'exploitation des données copiées, lorsque cela est nécessaire, les délais prévus à l'alinéa précédent peuvent être prorogés, pour la même durée, par le juge des référés saisi par l'autorité administrative au moins quarante-huit heures avant l'expiration de ces délais. Le juge des référés statue dans un délai de quarante-huit heures sur la demande de prorogation présentée par l'autorité administrative. ***Si l'exploitation ou l'examen des données et des supports saisis conduisent à la constatation d'une infraction, ils sont conservés selon les règles applicables*** *en matière de procédure pénale.*

Pour l'application des dispositions du présent article, le juge des référés est celui dans le ressort duquel se trouve le lieu de la perquisition. Il statue dans les formes prévues au livre V du code de justice administrative, sous réserve des dispositions du présent article. ***Ses décisions sont susceptibles d'appel*** *devant le juge des référés du Conseil d'État dans un délai de 48 heures à compter de leur notification. Le juge des référés du Conseil d'État statue dans le délai de 48 heures. En cas d'appel, les données et les supports saisis demeurent conservés dans les conditions mentionnées au huitième alinéa du présent article.* »

Dans ces conditions, il paraît vraisemblable qu'en cas de contestation, le Conseil constitutionnel ne trouvera rien à redire à la copie des données réalisées par les policiers.

Article original de Guillaume Champeau

Réagissez à cet article

Original de l’article mis en page : État d’urgence et copie des données informatiques : le cadre prévu par le gouvernement – Politique – Numerama

---

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

Envoyez désormais des fichiers aux contacts hors ligne avec Skype

---

La mise à jour de Skype permet de transmettre des fichiers aux contacts hors ligne. En outre, la limite maximale par fichier a été relevée à 300 Mo.

Si vous avez l'habitude d'envoyer des fichiers par Skype, voilà une nouvelle qui devrait vous satisfaire : en récupérant la version la plus récente du logiciel de téléphonie et de messagerie instantanée, vous pouvez partager des contenus lorsque les destinataires ne sont pas connectés au moment de l'envoi.

Cette fonctionnalité implique manifestement un stockage du fichier sur les serveurs de Microsoft – la maison-mère de Skype – afin que le service puisse être en mesure de le faire suivre quand le destinataire se reconnectera. L'envoi peut concerner un seul contact ou tout un groupe de discussion.

Attention, néanmoins. Une limite à 300 Mo par fichier est appliquée par Microsoft. Si celle-ci suffit amplement dans la plupart des cas, vous ne pourrez pas envoyer une vidéo trop lourde. Il faudra procéder autrement si vous tenez absolument à envoyer ce fichier qui contient « 2016.TRUEFRENCH.EXTENDED.BDRip.XViD.AC3 » dans le titre…

Une autre évolution appréciable de Skype figure dans l'accès à un fichier depuis de multiples appareils. Maintenant, vous pouvez lire le même document depuis votre smartphone, votre tablette ou votre ordinateur, sans avoir besoin de demander à votre interlocuteur de vous le renvoyer.

Article original de Julien Lausson

Réagissez à cet article

Original de l'article mis en page : Skype vous permet d'envoyer des fichiers aux contacts hors ligne – Tech – Numerama

L’Internet russe prêt à ériger des frontières

L’Internet russe prêt à ériger des frontières

La Russie prévoit de contrôler davantage la partie russe du réseau Internet et son trafic, y compris l'activité des serveurs DNS et l'attribution des adresses IP.

L'an dernier, la Russie a annoncé l'entrée en vigueur d'une loi obligeant toute organisation détenant des données de citoyens russes à les stocker sur des serveurs se trouvant physiquement sur le territoire russe. Cette année, un autre projet de loi concocté par le ministère russe des communications, prévoit la création d'un système de surveillance du trafic Internet, y compris l'activité des serveurs DNS (système de noms de domaine) et l'attribution des adresses IP.

Le texte, dont le journal *Vedomosti* s'est fait l'écho, vise à réguler *« la partie russe du réseau Internet »*. Et ce officiellement pour renforcer la protection de l'Internet russe face aux cyberattaques. Le projet implique aussi la surveillance du trafic Internet transfrontalier, en s'appuyant notamment sur le système SORM (système pour activité d'enquête opératoire). Reste à savoir si la Russie a les moyens de faire appliquer de telles restrictions, dont elle devra mesurer l'impact économique.

Réseau de réseaux

Dave Allen, vice-président et avocat général de Dyn, un spécialiste de la performance réseau basé dans le New Hampshire, aux États-Unis, a publié une tribune sur le sujet dans *Venturebeat*. Allen observe qu'une grande partie du trafic Internet russe dépend actuellement beaucoup de pays avec lesquels la Russie entretient des relations compliquées, voire conflictuelles.

Les données partagées de Moscou à Saint-Pétersbourg par un abonné de l'opérateur mobile russe MegaFon, par exemple, transitent 9 fois sur 10 par Kiev, en Ukraine, selon lui. Et plus de 40 % des données qui passent par le réseau de MTS, le premier opérateur mobile russe, pour aller aussi à Saint-Pétersbourg, transiteraient par Amsterdam aux Pays-Bas et par Francfort en Allemagne.

La tendance se vérifie auprès d'entreprises publiques : ainsi, plus de 85 % des données transmises de Moscou vers Saint-Pétersbourg par TransTelekom, filiale de la Compagnie des chemins de fer russes, passeraient par Francfort. Et la plupart des données qui quittent la Russie, selon Dave Allen, passent par le backbone RETN, qui a des points de présence en Europe centrale et orientale.

Localisation de données

Les mesures de renforcement de la protection des données russes s'appliquent à toutes les entreprises ayant une activité dans le pays. L'an dernier, le régulateur russe Roskomnadzor a mené un audit auprès de 317 sociétés et administrations. Il a estimé que 2 étaient dans l'illégalité. L'audit pourrait être étendu cette année à d'autres grands groupes, dont Microsoft, HPE et Citibank.

Pour que les données puissent être transférées temporairement à l'étranger, une protection *« adéquate »* de ces données doit exister. L'Ukraine, l'Allemagne et les Pays-Bas ont signé une convention sur le traitement automatisé de données personnelles qui semble satisfaire cette condition. En revanche, le doute persiste sur le chiffrement. Le gouvernement russe, comme d'autres, envisage de l'affaiblir pour donner plus de marge de manoeuvre à ses services de renseignement.

D'autres pays ont fait des propositions en faveur de la localisation de données. En France, un amendement qui prévoyait l'interdiction de traitement de données personnelles stockées hors d'un État membre de l'Union européenne, a finalement été écarté du projet de loi République numérique.

Article original de Ariane Beky

Réagissez à cet article

Original de l’article mis en page : L’Internet russe prêt à ériger des frontières

---

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

Peut-on vraiment forcer les collectivités locales d’utiliser un « cloud souverain » ?

---

par Emilien Ercolani

Une circulaire d'avril dernier, qui sert à rappeler le cadre légal applicable, écrit noir sur blanc qu'il est illégal d'utiliser « un cloud non souverain » pour les documents créés et gérés par les collectivités territoriales. Au-delà d'être illusoire, la mesure est en plus ubuesque.

C'est une circulaire du 5 avril 2016 qui a remis le sujet sur le tapis. Relative à l'informatique en nuage, elle explique tout d'abord que les documents et données numériques produits par les collectivités territoriales « *relèvent du régime juridique des archives publiques dès leur création* ». Les archives publiques sont considérées comme « *des trésors nationaux* », et les données numériques ne font pas exception.

Le raisonnement est donc le suivant : pour protéger les « *trésors nationaux* », il convient de les conserver sur le territoire national pour ainsi dire garantir leur préservation. « *Un trésor national ne peut pas sortir du territoire douanier français sinon à titre temporaire* », souligne encore le texte. Pour les données numériques, il faut donc qu'elles soit traitées et stockées en France. Raisonnement logique… pour qui ne connaît pas vraiment le monde de l'informatique.

Les conséquences de la loi appliquée à la lettre

Concrètement, cela voudrait dire qu'une collectivité territoriale doit donc traiter et stocker ses données, anciennes et futures, sur le territoire. Et donc, dans des data centers installés sur le sol français. Ce qui implique que toutes les suites d'outils logiciels et bureautiques en mode cloud sont désormais interdites : Office 365 et les Google Apps (pour ne citer que les plus connues) sont désormais bannies puisque ni l'une ni l'autre ne sont en mesure de garantir un stockage sur le territoire national.

« *L'utilisation d'un cloud non souverain (…) est donc illégale pour toute institution produisant des archives publiques* », poursuit la circulaire. A savoir que la définition d'un cloud souverain pour la direction générale des collectivités locales (DGCL), qui dépend du ministère de l'Intérieur, est la suivante :

Modèle de déploiement dans lequel l'hébergement et l'ensemble des traitements effectués sur des données par un service de cloud sont physiquement réalisés dans les limites du territoire national par une entité de droit français et en application des lois et normes françaises.

Une circulaire « politique »

La circulaire s'appuie toutefois sur des textes de loi, et notamment sur les articles L211-1 et L211-4 du Code du Patrimoine, utilisés dans le Référentiel général de gestion des Archives. Mais, concrètement, cela traduit d'une part une méconnaissance de l'informatique en règle générale, d'autre part des mesures qui ne sont pas réalistes.

Responsable juridique du Syntec Numérique, Mathieu Coulaud nous explique tout d'abord que cela ne pénalise pas que Google ou Microsoft, mais aussi des acteurs européens ; l'Allemand T-Systems héberge par exemple de nombreuses données des collectivités territoriales françaises. D'autre part, il s'étonne « qu'aucune consultation et d'étude d'impact n'aient été réalisées ». Pour lui, cette circulaire est donc purement politique dans le sens où :

• Rien n'a été fait pour ouvrir le dialogue et s'informer des conséquences d'une telle mesure

• Cela dénote une incompréhension de la part des pouvoirs publics mais aussi les dissonances entre les différents ministères

« Nous avions écrit au directeur du SIAF (Service Interministériel des Archives de France) en 2015. Nous avons reçu sa réponse en janvier 2016, qui était en somme une fin de non-recevoir », poursuit Mathieu Coulaud. « Pour nous, ils confondent sécurité et localisation des données ». Effectivement, car même l'Anssi ne semble pas avoir été consultée, elle qui prépare un label « Secure Cloud » sensé garantir la souveraineté des données hébergées.

***Exclusif** : ce mercredi 6 juillet a lieu une réunion interministérielle qui réunit notamment Bercy, Matignon et le ministère de la Culture. Les administrations vont donc se parler et le sujet sera vraisemblablement à l'ordre du jour.*

« Nous avons déjà été reçus par différents ministères (Economie, Culture, etc.) mais sans rien obtenir. Plusieurs recours sont possibles, notamment concernant l'accès à la commande publique. Nous estimons qu'il existerait avec cette circulaire une vraie discrimination entre les acteurs, ce qui est contraire à la loi. Le ministère de la Culture assure que tout est viable juridiquement, mais je n'ai rien pu vérifier », ajoute Mathieu Coulaud qui souligne : « nous nous réservons des actions possibles d'influence et de droit ».

Une double lecture

Le rappel du cadre légal a rapidement fait réagir de toutes parts. « Je ne peux m'empêcher de penser qu'il s'agit de fausses bonnes nouvelles pour les prestataires de services comme pour les collectivités locales », estime Christophe Lejeune, directeur général de l'entreprise nantaise Alfa Safety qui persiste : « Enfermer dans un cadre strictement national un service innovant comme le cloud est un contre-sens ». Pour le Syntec Numérique, la circulaire va à rebours du projet de loi République Numérique, crée des barrières protectionnistes et freinera la transformation numérique. Sans compter qu'elle ne dit rien sur la nature des données en elles-mêmes. « Si un DSI envoie un smiley, cela devient un trésor national !« , ironise Mathieu Coulaud.

Mais à bien y regarder, la circulaire en question n'est-elle pas fondamentalement positionnée pour défendre les enjeux nationaux ? Et pourquoi pas faire émerger un nouveau « cloud souverain » français, voire des alternatives logicielles en mode cloud ? Opportuniste, l'hébergeur du Nord OVH rappelle non seulement son implantation en France mais aussi ses certifications et finalement qu'il est un « acteur national responsable, capable d'héberger sans risque les données issues du travail et des archives des différentes institutions publiques ; créant ainsi un Cloud véritablement souverain et fonctionnel ».

Réagissez à cet article

Original de l’article mis en page : Les collectivités locales forcées d’utiliser un « cloud souverain » ?

L’Etat français (ANSSI) va certifier les Cloud de confiance

	L’Etat français (ANSSI) va certifier les Cloud de confiance

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.

L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « *Huit prestataires se sont lancés dans ce processus de qualification* », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « *La qualification n'est pas un outil de protectionnisme* », reprend Guillaume Poupart. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi.
Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 001.

Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +… Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : les Américains out ?

« *Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients* », explique Laurent Seror, le président d'Outscale, le fournisseur de Iaas né sous l'impulsion de Dassault Systèmes. « *Etant donné que nous sommes déjà certifiés ISO 27 001, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision* », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « *On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes.* »
La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Axelle Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « *Cet amendement n'était pas téléguidé*, assure aujourd'hui Guillaume Poupard. *Je l'ai découvert au moment des débats.* » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.
Article original de Reynald Fléchaux

Réagissez à cet article

Original de l'article mis en page : L'Etat français va certifier les Cloud de confiance

Cloud et sécurité : le point sur 7 questions qui fâchent

	Cloud et sécurité : le point sur 7 questions qui fâchent

Le nuage informatique est à la mode chez les grands comptes, mais aussi chez les PME et TPE qui n'hésitent plus, parfois, à y déverser des données sensibles. La prudence reste pourtant de mise.

En France, le marché du "cloud" n'est pas encore mature », confie Henry-Michel Rozenblum, délégué général d'EuroCloud France, l'association des fournisseurs français de « cloud » liée à la fédération européenne Eurocloud. Ce qui signifie qu'il n'y a pas de standard de sécurité spécifique. L'approche consiste plutôt à s'appuyer sur les bonnes pratiques traditionnelles de la sécurité informatique. Notamment la certification ISO 27001, qui, si elle est délivrée par un grand cabinet d'audit, est la seule garantie qui fait foi. Autrement, pas de véritable sécurité. *« Même si le discours marketing prétend le contraire »,* souligne Gérôme Billois, expert sécurité au Cercle européen de la sécurité et des systèmes d'information.

Les pirates s'adaptent

Il existe sur Internet, des « black markets » électroniques (places de marché pirates), où des logiciels clefs en main s'échangent sans contrôle. Ils permettent de mener des attaques complexes contre un « cloud », sans même avoir besoin de solides compétences en informatique. Leur nom : des « hyperkits ». *« En quelques clics, ils permettent de prendre le contrôle d'un serveur physique à partir du serveur virtuel »,* prévient Jean-Paul Smets, PDG de Vifib, un offreur de « cloud » distribué. *« L'unique manière de s'en protéger est de maintenir son système à jour et de combler systématiquement les failles de sécurité. »*

Un risque systémique

En dehors des attaques, rappelons que le **cloud est, lui-aussi, sensible aux bugs, pannes et erreurs humaines…** *« Comme une poignée d'opérateurs de "cloud" domine le marché, le moindre problème prend une ampleur démesurée »,* explique Gabriel Chadeau, directeur commercial chez Vision Solutions, spécialiste de la récupération de données. Normal : lorsque le nuage « plante », des milliers d'entreprises n'accèdent plus à leurs services. Pour se protéger, il faut se demander quels services externaliser dans le « cloud » et quels autres garder chez soi. *« Je déconseille de mettre ses applications métiers dans le cloud. Pour des raisons de disponibilité et de confidentialité »,* souligne Gérôme Billois.

Une confidentialité illusoire

Pour de nombreux acteurs, la **confidentialité est le point noir du cloud computing**. Les fournisseurs américains sont particulièrement visés par les critiques. Car le **Patriot Act les oblige ainsi que leurs filiales situées en dehors des Etats-Unis à remonter des données vers leurs autorités**. En novembre 2012, le rapport « cloud computing » dans l'enseignement supérieur et les instituts de recherche et le Patriot Act américain, rédigé par des juristes de l'université d'Amsterdam, expliquait qu'il s'agissait d'un droit *« extraterritorial »* et qu'il ne s'embarrasse pas des lois nationales ou européennes… En ce moment, l'Europe légifère sur le sujet. En attendant, mieux vaut se rabattre sur un offreur cloud français.

De l'espionnage en interne

Reste qu'un fournisseur français n'est pas un gage de sécurité en soi. *« Parce que, lorsqu'une donnée circule dans le nuage, des centaines de techniciens y ont accès. Par le jeu de la sous-traitance, plus de la moitié d'entre eux ne sont pas en France »,* assure Hervé Schauer, membre du Club de la sécurité de l'information français (Clusif) et expert en sécurité des systèmes d'information. *« Si l'une de ces personnes est corrompue, il n'y a plus de confidentialité dans le cloud. »* Pour se prémunir, il faut obliger son fournisseur à apporter des garanties concrètes. *« Il doit pouvoir expliquer comment son architecture est techniquement cloisonnée et comment les droits sont gérés »,* explique Matthieu Bennasar, consultant sécurité au Lexsi, un cabinet spécialisé en sécurité informatique et gestion des risques.

Chiffrement faible

A défaut d'obtenir ces garanties, il faut vivre avec la crainte d'être mis sur écoute, dans le nuage. Et le bon vieil argument qui veut que le chiffrement protège efficacement les données contre les regards malveillants ne tient en réalité pas la route. C'est un écran de fumée. *« Aucun chiffrement n'est infaillible »,* rappelle Patrick Debus-Pesquet, directeur technique chez Numergy, un des deux opérateurs de cloud souverain. Ce qu'il faut faire, souvent, c'est auditer son cloud afin de déceler la présence de sondes et de logiciels espions.

Pas d'audit par défaut

Mais encore faut-il pouvoir auditer son cloud ! Tous les offreurs ne le permettent pas. *« Il faut négocier en amont une clause d'auditabilité, c'est indispensable »,* martèle Philippe Hervias, directeur sécurité à l'Institut français de l'audit et du contrôle interne (Ifaci).

Réversibilité impossible

Dans tous les cas, négocier avec son fournisseur est une stratégie gagnante. Dans le cas inverse, le risque est de se retrouver piégé avec un mauvais prestataire. Et de ne pas pouvoir en changer, parce qu'il est difficile – voire impossible – de réinjecter ses données dans un nouveau système d'information. *« Je n'ai jamais vu un tel principe mis en œuvre »,* admet Pierre-Josée Billotte, président du conseil d'administration d'Eurocloud France. Il faut donc redoubler de vigilance au moment de signer son contrat. Ou choisir exclusivement des applications SaaS à base de logiciels libres que l'on peut répliquer gratuitement sur une autre plate-forme.

Article original de GUILLAUME PIERRE

Réagissez à cet article

Original de l'article mis en page : Cloud et sécurité : le point sur 7 questions qui fâchent – Les Echos Business

---

Facebook regarde dans quels

magasins vous faites vos courses

	Facebook regarde dans quels magasins vous faites vos courses

Facebook va désormais traquer les données de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but est de permettre aux annonceurs de savoir si leurs publicités attirent des consommateurs sur leurs points de vente.

Facebook ne cesse de renforcer son service de publicités. Le réseau social veut proposer une offre plus précise et pertinente pour ses clients. Pour cela, il se servira désormais des données de localisation de ses utilisateurs pour savoir dans quels magasins ils se rendent. Le but ? Permettre aux entreprises de savoir si leurs annonces sur Facebook attirent du monde dans leurs magasins.

Ainsi, les annonceurs pourront comparer le nombre de personnes qui ont vu leurs annonces au taux de fréquentations de leurs points de vente. Ils peuvent également intégrer une carte interactive à leur publicité – sous la forme d'un carrousel – pour indiquer à l'internaute le chemin qui le mènera au magasin le plus proche.

Ces nouvelles fonctionnalités s'inscrivent dans une volonté de Facebook de proposer des services plus personnalisés – et donc plus efficaces – à ses clients. En 2014, la boîte de Mark Zuckerberg avait déjà lancé une plateforme qui permet d'afficher de la publicité aux utilisateurs du réseau social qui se trouvent à proximité du magasin afin de les inciter à s'y rendre rapidement.

Selon Facebook, plusieurs entreprises ont déjà eu l'occasion de tester, en avant-première, ces nouvelles fonctionnalités. Parmi eux, se trouve E.Leclerc. La chaîne de distribution française « a pu atteindre 1,5 millions de personnes dans un rayon de dix kilomètres autour de ses supermarché et a observé qu'environ 12 % des clics sur leur publicité ont entraîné une visite en magasin dans les sept jours qui suivaient », indique Facebook dans son annonce.

Grâce à ces jeux de données très précis, Facebook fournit des outils pertinents pour les entreprises car, grâce à cela, elles peuvent ajuster leur stratégie de communication en fonction de chaque point de vente et de chaque région. Le réseau social prouve encore plus à quel point il représente un atout bien plus puissant que les modes de diffusion traditionnels.

Quant aux utilisateurs de Facebook, si cette information a de quoi énerver, elle n'a rien de vraiment surprenant. Il est de notoriété publique que la publicité ciblée représente le fonds de commerce principal du réseau social. Celui-ci n'est d'ailleurs pas le seul à traquer les internautes pour savoir dans quels magasins ils vont. Google le fait depuis quelques temps déjà, comme le rappelle, dans un tweet, Jason Spero, responsable de la stratégie et des ventes mobiles chez la firme de Moutain View.

Google dispose de données encore plus importantes destinées aux annonceurs et adapte les publicités en fonction, entre autres, des recherches de l'utilisateur et de sa géolocalisation.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Facebook regarde dans quels magasins vous faites vos courses – Business – Numerama

Cloud souverain : les collectivités locales ne pourront pas y couper

	Cloud souverain : les collectivités locales ne pourront pas y couper

Dans une circulaire publiée au Journal Officiel, le Ministère de la Culture indique que les collectivités locales françaises devront passer par des prestataires hébergés en France pour traiter les données relatives aux citoyens français.

Mieux vaut tard que jamais : une circulaire parue au Journal officiel et signée par la direction générale des collectivités locales et le service interministériel des Archives de France vient clarifier les dispositions relatives au « cloud souverain ». Le texte, repérée par NextInpact, explique que les collectivités françaises devront impérativement passer par des prestataires situés sur le territoire français pour stocker et traiter les données dans le cloud.

Le texte se veut une clarification des directives données dans le cadre du « Guide sur le cloud computing et les datacenters à l'attention des collectivités locales. » La circulaire précise notamment le statut des données produites par les collectivités territoriales. Celles-ci « relèvent du régime politique des archives publiques dès leur création. ».

Point de salut

Outre cet aspect, la circulaire précise quelques lignes plus loin que « toutes les archives publiques sont par ailleurs des trésors nationaux en raison en raison de l'intérêt historique qu'elles présentent ou sont susceptibles de présenter. » Un régime qui s'applique autant aux documents physiques qu'à leurs équivalents numériques et qui implique une nécessaire localisation des données sur le territoire national. Celle-ci ne peut être contournée qu'à titre temporaire sur une demande adressée directement au ministère de la Culture.

Hors des fournisseurs de cloud souverain, point de salut pour les collectivités qui souhaitent avoir recours à ce type de service. La circulaire donne également une définition de ce que l'administration entend par cloud « souverain » : un « cloud dont les données sont entièrement stockées et traitées sur le territoire français. » La circulaire précise également que l'Anssi travaille sur la production d'une offre de labellisation des offres qui répondent à ces critères, label baptisé « Secure Cloud ».

Initié en 2014, le label n'est pas encore entièrement opérationnel et est encore en « phase d'expérimentation » jusqu'à la moitié de l'année 2016 selon le site de l'Afnor. Celui-ci devrait donc sous peu être en mesure de proposer une liste de fournisseurs qualifiés pour répondre aux besoins des collectivités locales en matière de services cloud.

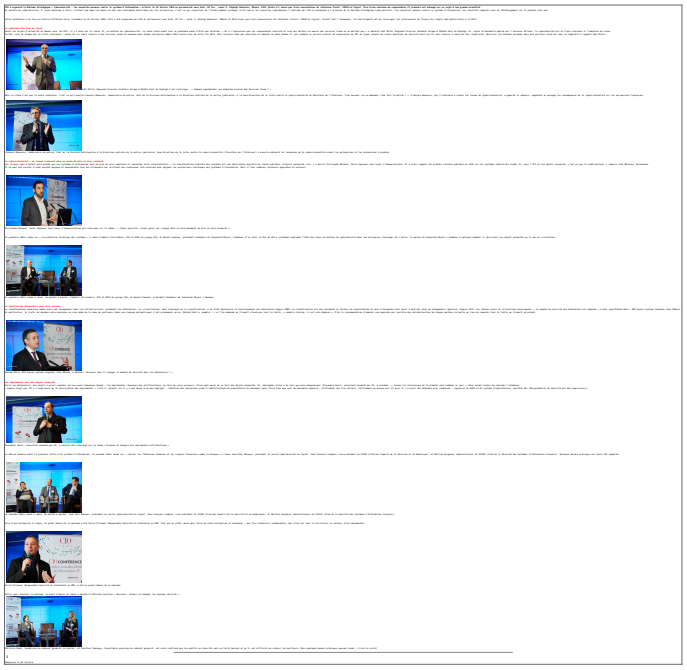
Article original de ZDNet

Réagissez à cet article

Original de l'article mis en page : Cloud souverain : les collectivités locales ne pourront pas y couper – ZDNet

Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

Safe Harbor & Privacy Shield : Comment l'entreprise peut avoir le contrôle complet de son propre cloud ?

L'invalidation de l'accord Safe Harbor a provoqué une certaine incertitude chez de nombreuses entreprises qui ne savent plus comment sauvegarder leurs données en toute sécurité et légalité – tout en les mettant à la disposition de leurs collaborateurs.

Début février, l'accord Safe Harbor 2.0 – surnommé Privacy Shield – a vu le jour, mais de nombreux doutes sur sa légitimité subsistent.
Dans ce contexte, l'incertitude demeure au sein des entreprises qui se posent de nombreuses questions autour de la conformité et ne savent pas si le Privacy Shield sera une solution sur le long terme. Il est toutefois possible de contourner les problématiques liées à l'instabilité de telles réglementations en trouvant la bonne solution – ainsi qu'un fournisseur de services adapté.

Il existe deux alternatives pour sauvegarder et utiliser ses données en toute sécurité dans le cloud sans se soucier de problématiques de conformité.
D'une part, l'entreprise peut rechercher un fournisseur de cloud computing exploitant ses Data Centers dans un pays européen. D'autre part, les entreprises sont tout à fait capables de constituer leur propre cloud et d'y mettre leurs données, ressources informatiques et applications à la disposition de leurs collaborateurs. Le marché du stockage externe offre de nombreuses solutions pour ces deux approches. Le rôle, pour tous les grands acteurs sur le marché, étant d'offrir aux clients une sauvegarde et un partage parfaitement sûrs de leurs données dans le cloud.

Les utilisateurs du cloud doivent pouvoir faire entièrement confiance à leur fournisseur de services
Dès qu'une entreprise prend la décision d'utiliser une architecture cloud public pour stocker une partie de ses informations, elle doit trouver un fournisseur adapté à ses exigences mais également irréprochable en termes de fiabilité.
La priorité dans cette démarche, lorsque l'on souhaite éviter des soucis de conformité, est de s'assurer que le fournisseur mette à disposition ses centres de données en Europe. En outre, l'entreprise est parfaitement en droit de demander si la sauvegarde de données de son fournisseur est effectuée exclusivement dans ses propres centres de données ou s'il en fournit une copie à d'autres centres de données d'un pays tiers. L'évaluation des accords de niveau de service (SLA), de la méthode et de la chronologie de sauvegarde appliquée pour telles ou telles données mais aussi des conditions de leur récupération sont des points à examiner lors du choix du fournisseur.
Cela permet d'établir une solution de confiance entre l'utilisateur et son service cloud. C'est sur la base de cette confiance et de la garantie que leurs données ne quittent pas l'Europe que les utilisateurs peuvent opter pour différents services de cloud.
D'autre part, l'utilisateur doit impérativement veiller à ce que le fournisseur utilise un encodage afin d'écarter tout risque d'utilisation abusive (intentionnelle ou aléatoire) de ses données.

L'entreprise peut avoir le contrôle complet de son propre cloud
La deuxième option garantie une sauvegarde et un partage des données parfaitement sûrs dans une architecture cloud, et confère donc à l'entreprise le plein contrôle sur ses informations et services numériques. Légèrement plus complexe, cette option consiste à créer sa propre architecture cloud privée.
L'entreprise devra certes gérer davantage de ressources, mais elle pourra puiser pleinement dans les services mis à disposition, les droits d'accès, la sélection des applications et l'assistance technique. Ces avantages garantiront une meilleure flexibilité aux collaborateurs de l'entreprise, ainsi que des outils nécessaires pertinents pour faciliter leurs tâches et les mêmes droits d'utilisation que s'ils travaillaient dans un cloud public. La sécurité des données et des appareils sera également garantie conformément aux mesures internes prises par l'entreprise.
Un cloud privé n'est pas concerné par les effets de Privacy Shield et permet d'utiliser différents services basés sur le cloud computing. En effet, les applications telles que « Box » ou « Dropbox » ne devraient plus être utilisées dans un environnement influé par de telles réglementations.

La pratique BYOD est une tendance très actuelle dans le monde de l'entreprise, mais elle complique l'intégration des terminaux dans les procédures de sauvegarde et rend difficile un contrôle complet sur toutes les informations de l'entreprise. L'utilisation combinée d'un cloud privé et de solutions d'accès, de synchronisation et de partage des fichiers est susceptible de remédier à cela. Les collaborateurs pourront ainsi accéder en toute sécurité aux données depuis n'importe quel terminal, les synchroniser et les partager avec leurs collègues, clients, partenaires et fournisseurs.
Un tel logiciel peut remplacer le serveur FTP et permet, par exemple, le libre-service en créant différents comptes utilisateurs tout en déchargeant les tâches de l'administrateur. L'intégration de solutions MDM facilite la gestion des appareils portables et assure un contrôle souple des données et des comptes.
Via l'utilisation d'une bonne solution d'accès, de synchronisation et de partage, le responsable informatique peut mettre en place une meilleure gouvernance des données en établissant des droits d'accès mais peut aussi retracer le transfert ou le partage éventuels des données concernées.
Les entreprises désireuses d'utiliser un cloud parfaitement sûr et de conserver le plein contrôle de leurs ressources et données opteront donc pour un cloud privé et des applications adaptées aux besoins de leurs collaborateurs et personnel informatique.

La sécurité doit être la priorité absolue
La débâcle provoquée par l'invalidation du Safe Harbor a permis de tirer une leçon très importante. La sécurité et la confidentialité des données doivent être des priorités absolues, quelle que soit la solution choisie par une entreprise, qu'il s'agisse d'un cloud privé ou public. Les informations numériques doivent donc impérativement être encodées avant de quitter l'entreprise ou – mieux – le réseau protégé. Une procédure de sauvegarde, par exemple, offre déjà une certaine protection, mais pour toutes les entreprises désireuses d'empêcher définitivement tout accès illicite à leurs données personnelles ou d'entreprise, l'encodage est une priorité absolue. Seul un encodage efficace est apte à garantir la protection et la sécurité des données … [Lire la suite]

Réagissez à cet article

Source : *Safe Harbor & Privacy Shield : comment assurer la conformité ? – JDN*