Traçabilité et cartographie de la donnée au cœur de l'application du RGPD

On l'oublierait presque : le **Règlement général sur la protection des données (RGPD ou GDPR en anglais)** est dans les faits entré en vigueur le 25 mai 2016. Mais les Etats membres disposent d'un délai de deux ans pour l'adopter aux législations nationales. Son échéance d'application dans l'UE est donc fixée au 25 mai 2018.

« On est dans la phase où il est demandé à tout le monde de se mettre en conformité », confirme Olivier Iteanu, avocat au barreau de Paris.

Le spécialiste des nouvelles technologies constituait l'un des invités du débat « RGPD : le coût de la protection de la vie privée version européenne va-t-il plomber les entreprises ? » organisé mercredi 20 septembre matin par le Club de la Presse Informatique B2B de José Diz.

Si le RGPD est *« l'aboutissement du processus d'harmonisation européenne »* sur la protection des données *« personnelles »* – Olivier Iteanu insiste sur ce point – commencé en 1978 en France avec la création de la Cnil (Commission nationale de l'informatique et des libertés), le nouveau texte n'en constitue pas moins un règlement ambitieux que l'avocat résume en 5 points :
– des sanctions pouvant aller jusqu'à 4% du chiffre d'affaires mondial de l'exercice précédent de l'entreprise en cas de manquement;
-la fin de la déclaration à la Cnil au profit d'un système de responsabilité même si, objet d'un autre point, la Commission conserve un rôle majeur (*« les règles d'or de la Cnil continueront d'exister après le 25 mai 2018 »*);
– l'élargissement des responsabilités aux sous-traitants (*« ils sont justiciables devant la loi en plus du client »*);
– et le droit à l'oubli pour les citoyens étendu au droit à la portabilité des données et à l'action de groupe.

Localisation des données

La question du stockage des données en dehors des frontières européennes se pose plus que jamais dans le cadre du RGPD, particulièrement aux Etats-Unis.

Un faux débat puisque le Privacy Shield, du nom de l'accord entre l'Europe et les Etats-Unis qui succède au Safe Harbor (et en cours d'évaluation annuelle), encadre l'utilisation des données européennes par une entreprise américaine sur son sol.

« En théorie une entreprise comme Salesforce, par exemple, est justiciable au RGPD, considère l'avocat, *reste à savoir comment la Cnil va contrôler le respect du texte à l'étranger. »*

La question ne se posera peut-être bientôt plus. *« Je pense que les Gafam [Google, Apple, Facebook, Amazon, Microsoft], les grands acteurs du SaaS, finiront par s'installer dans chacun des pays [européens] pour rassurer les clients »*, considère Fabien Gautier.

Le directeur Business Development et Marketing chez Equinix rappelle que l'hébergeur est impliqué par le RGPD *« même si on ne touche pas à la donnée »*.

Implication de l'écosystème

D'abord par la sécurisation de la donnée, tant pour les infrastructures hébergées que la gestion des personnes qui évoluent dans le bâtiment et peuvent accéder aux serveurs. Mais surtout par le service qu'il apporte autour de la donnée et l'écosystème qu'elle génère.

« Nous avons une centaine de clients [en France, NDLR] et 12□000 interconnexions environ, illustre le responsable d'Equinix. *Les liens directs consomment deux fois plus de bande passante qu'Internet. »*

Une façon de souligner que les clients se rapprochent des uns des autres au sein du datacenter pour optimiser leurs échanges de données, ce qui ouvre à la création de nouveaux services et, donc, autant d'opportunités d'affaires. Mais qui implique une responsabilité sur la gestion de la donnée élargie à tout l'écosystème.

« Pour le DSI, le premier élément de réponse est le cheminement plus direct entre les différents acteurs », estime Fabien Gautier. Autrement dit, mieux vaut privilégier les liens d'interconnexion plus faciles à maîtriser que des liens Internet.

« Avec le RGPD, on demande à un contorsionniste de continuer à faire ce qu'il fait mais avec une armure. » Par cette allégorie, Jean-François Marie, EMEA Product and Alliance Director chez NetApp, entend rappeler que *« le Cloud hybride est une réalité qui s'impose aujourd'hui à toutes les entreprises »* et installe l'ambigüité au cœur des échanges. Quel traitement appliquer à la donnée□? En combien de temps□? Avec quelles ressources□?

« La donnée va être acheminée pour être disponible dans un Cloud mais le socle physique peut être éphémère, la donnée peut bouger du datacenter, explique le porte-parole du fournisseur de solutions de stockage. *Comment je conserve la conformité lors du transfert de la donnée□? »* Chez NetApp, la solution consiste à *« identifier les acteurs qui travaillent ensemble »*.

Une gestion quasiment impossible manuellement aujourd'hui qui oblige à recourir à l'automatisation. Ce qui implique *« un partenariat étroit entre les différentes parties dans les échanges technologiques pour garantir l'interaction des applications »*. Echanges qui passent par le recours massif aux API, essentiellement.

Automatiser au maximum

Ce n'est pas Valérie Lourme qui le contredira. *« Sécuriser la donnée par le design sans briser le business et à coût acceptable est un enjeu d'une extrême complexité. Difficile de le faire manuellement*, considère la consultante Industry Senior chez Teradata. *Il faut automatiser tout ce qui peut l'être. »*

Le spécialiste de l'entreposage de données propose une démarche d'évaluation des besoins en cartographiant la donnée de sa source à l'usage afin de mettre en œuvre une stratégie. Un mal pour un bien puisque cette démarche pousse à *« simplifier, rationaliser la gestion de la donnée, éviter les redondances inutiles [quitte à] supprimer des données »*. Bref, *« mieux urbaniser le système de données »*.

C'est justement sur le côté du système où la donnée est la plus utilisée, à savoir le poste de travail, qu'elle est le plus à risque. *« Car utilisée »*, souligne Bastien Bobe.

Pour l'ingénieur avant-vente, expert sécurité chez Ivanti, spécialiste de la sécurité applicative, la sécurisation de la donnée passe par la classification des applications et la gestion des droits d'utilisateurs à exploiter la donnée, y compris en mobilité.

« Les DSI ont du mal à savoir qui a besoin de la donnée, si elle peut être sortie de l'entreprise et comment la sécuriser ». Une problématique à laquelle peuvent répondre les solutions de gestion des identités.

Le casse-tête du droit à l'oubli

Outre la sécurisation de la donnée, se pose également la question du droit à l'oubli. Comment être sûr de supprimer des données personnelles à la demande d'un citoyen face au phénomène de duplication et redondance à travers les différents prestataires ?

Pour Jean-François Marie (NetApp), qui s'appuie sur l'exemple de l'Estonie, pays qui a instauré l'e-citoyenneté, *« la traçabilité [de la donnée] est peut-être la solution. Quand on a une seule source, c'est plus facile pour appliquer le droit à l'oubli »*.

Mais *« avoir une version unique de la donnée est impossible*, juge Valérie Lourme (Teradata), *c'est l'usage de la donnée qui importe pour garantir la cohérence du SI pour accéder à la données où qu'elle soit »*.

Néanmoins, aux yeux de Bastien Bobe (Ivanti), la traçabilité reste incontournable face aux obligations déclaratives en cas de fuites de données induites dans le GRPD. *« Savoir quelles données ont été perdues impose leur traçabilité. »*

De son côté, Fabien Gautier considère que le RGPD s'inscrit comme une opportunité de *« rationaliser et faire le ménage »*. Et de citer l'exemple d'un client du secteur pharmaceutique qui a supprimé 30 à 40% de ses 230 applications dans le cadre de sa mise en conformité avec le règlement européen. *« C'est un point positif. »*

Du positif, Olivier Iteanu en voit aussi. Pour lui, *« l'objectif est vertueux et l'Europe montre la voie »* au reste du monde. L'avocat rappelle que, à travers le RGPD, la donnée reste la propriété de l'utilisateur. Sur ce point, il considère *« qu'on est en avance sur les Etats-Unis car la confiance ne peut pas se faire sans ce concept de propriété personnelle ».*

Tout en poursuivant : *« Nous avons intérêt à concilier l'Europe, les Etats-Unis et la Chine pour aller vers la confiance »*. Il ne reste plus qu'à en convaincre les entreprises.

Lire également
La facture salée que le GDPR prépare aux entreprises
Données personnelles : Ouicar fait une sortie de route
Le numérique, un défi pour notre Etat de droit ?