



SPF Economie, P.M.E., Classes moyennes et Energie

Le Cloud Computing

Une opportunité pour l'économie en Belgique

Résumé du rapport délivré par Unisys Belgium

Le *cloud computing* est l'accès à des ressources informatiques sur demande par l'intermédiaire d'un réseau.

C'est donc principalement un service dans lequel le client (l'utilisateur du *cloud*) utilise à distance des ressources qui lui sont fournies (plutôt que de tout installer localement chez lui).

Il y a plusieurs modèles de déploiement du service : privé (si le client est seul utilisateur des ressources qui lui sont dédiées), partagé (avec une communauté plus ou moins grande), public (quand le service est proposé à tous), étant entendu que ces modèles peuvent se mélanger de façon hybride.

Le service lui-même peut couvrir ou combiner diverses offres : l'infrastructure assurant calcul, stockage, back-up, bande passante (IaaS), la plateforme d'exploitation (PaaS) permettant enfin d'offrir en ligne des applications ou logiciels (SaaS) qui permettent de traiter des données.

Le principe économique du *cloud* évite au client de gros investissements en capitaux requis pour créer et maintenir une informatique de pointe (il peut avantageusement se consacrer à développer sa mission spécifique) et lui permet de payer les services (coûts opérationnels) uniquement s'il en a besoin et au moment où il en a besoin. Il faut aussi signaler que certains services, principalement destinés au grand public, sont « gratuits en contrepartie de publicité », comme le courrier électronique, les réseaux sociaux ou la recherche sur internet.

Le principe contractuel du *cloud*, au fur et à mesure que l'on va du « *cloud* privé » au « *cloud* partagé ou public » va d'un contrat négocié à un contrat par adhésion (dans lequel les conditions sont à prendre ou à laisser, et peuvent parfois même être modifiées unilatéralement par le fournisseur), ce qui renforce la nécessité de mettre en place un « cadre équitable ».

Le principe technique du *cloud*, qui est l'utilisation à distance, suppose la mobilité des données (dans les centres de calcul du fournisseur qui disposent au moment voulu de la puissance requise) et peut donc induire une perte de contrôle du client sur le lieu exact où elles sont conservées.

Les avantages du *cloud*, en plus de la création de nouveaux emplois dans les zones d'installation des centres de calcul (nouvelle branche d'activité compensant certaines pertes d'emploi ou réorientations au sein des clients) découlent de son principe économique et comprennent en outre pour les clients une meilleure gestion/attribution des coûts de chaque tâche, une agilité de prise décision (sans délais ni gestion prévisionnelle), une meilleure résistance face aux menaces cybernétiques et/ou sinistres (incendies, inondations, vols) qui peuvent affecter une informatique isolée, localisée en un seul point.

Les risques n'ont cependant pas disparu et – du fait de la taille des centres qui peuvent héberger les données de milliers de clients, soit des pans entiers d'une économie - ils ont pris une nouvelle dimension avec le *cloud*. La section 4 du rapport¹ les analyse selon le modèle de service (IaaS, PaaS, SaaS) et de déploiement (privé, public, hybride) et propose une approche d'évaluation des risques, de revue des politiques de sécurité du client, de traitement des risques et d'usage contrôlé du *cloud* avec des vérifications périodiques.

Le marché du *cloud* a fait, durant l'année écoulée, l'objet d'études nombreuses : il serait en croissance forte, passant en Europe, pour le *cloud* public ou communautaire de 4,6 milliards d'euros (2011) à 6,2 milliards d'euros pour 2012 (soit 34,8 % pour cette seule année). La part belge de ce marché est estimée à 2,5 %, soit 153 millions en 2012. La croissance peut avoir un aspect conjoncturel (les entreprises sont en recherche d'économies) et son maintien ou son évolution dépendra autant de la situation économique globale (reprise, sortie de crise ou non), que de l'absence d'incidents majeurs (pas de publicité négative) et de la dissipation des freins, incertitudes et manques de confiance vis-à-vis du *cloud*. Ce manque de confiance existe de la part des entreprises (spécialement les petites) mais aussi de la part du secteur public qui pourrait utiliser le *cloud*.

C'est dans ce dernier domaine que l'autorité régulatrice peut jouer un rôle important, selon qu'elle (et les opérateurs concernés) collabore ou non pour adopter un cadre juridique assurant une confiance forte du marché. On peut tracer trois scénarios : pessimiste, linéaire ou optimiste, selon lesquels le marché belge n'évoluerait d'ici 2020 que modérément (880 millions d'euros), linéairement (1,5 milliard d'euros) ou plus fortement (2 milliards d'euros en 2020).

Comment définir ce nouveau cadre juridique ? Les lois belges actuelles n'ont pas été formulées en tenant compte du *cloud* computing, et – au moins depuis la directive 95/46 –

¹ [Le Cloud Computing. Une opportunité pour l'économie en Belgique](#)

découlent du droit européen, l'intérêt pour un Etat membre de légiférer seul est ainsi limité. Si les rôles des partenaires du *cloud* (client et fournisseur) peuvent déjà être déduits du droit actuel (responsable du traitement et sous-traitant), le droit relatif au *cloud* va être influencé par une série de réformes européennes ou d'actions en cours :

- Un nouveau règlement général sur la protection des données (projet dévoilé en 2012) qui sera directement applicable (sans lois nationales) ;
- Une adaptation des droits du consommateur de confier au *cloud* ses copies privées et d'obtenir des clauses contractuelles équitables ;
- Une adaptation des règles relatives au commerce électronique et à la gestion du « contenu illégal » constaté sur le *cloud* ;
- Une définition des standards du « *cloud* européen » sur le plan technique (pour en assurer la portabilité), contractuel (pour un SLA équitable) et de la sécurité (rapport d'incidents, mesures et audit) ;
- Un « partenariat européen pour le *cloud* » qui vise non à construire un « super centre de *cloud* européen » mais à définir ces règles et standards communs permettant d'harmoniser les spécifications (notamment du secteur public) et les droits face aux offres des fournisseurs.

Toutes ces réformes ou actions (parfois devancées de manière fort isolée par les initiatives purement nationales de certains Etats) seront accompagnées d'études et de rapports (dont plusieurs sont en cours d'élaboration et attendus en 2013-2014). Elles ne seront pas appliquées du jour au lendemain, cela prendra des années.

Que peut donc faire l'autorité régulatrice belge ?

Elle doit d'abord s'inscrire dans l'approche européenne, pratiquant à cet égard une **veille technologique**, élaborant des documents de synthèse qui soient rapidement évolutifs, et en déclarant son ouverture à toute approche de **mutualisation** (pooling) de projets *cloud* avec les services publics de ses voisins.

Il faut que s'établisse une **relation de collaboration** avec les représentants de la profession du *cloud*, qui eux-mêmes doivent parvenir à une **meilleure organisation**, plus structurée et représentative de l'ensemble du secteur à travers les différentes régions et spécialisations.

Il est recommandé de devancer les conclusions attendues dans le cadre d'études en cours et du partenariat européen pour le *cloud* en élaborant, sur base des travaux de la Commission, de cette étude et des travaux du groupe de travail « Article 29 » une « version 1 » des **conditions contractuelles équitables** et prendre ainsi le leadership d'un label « **Fair Cloud** » qui sera ouvert à de nouvelles adhésions (fournisseurs de Belgique, du Benelux, d'autres Etats membres).

Le travail d'information doit se concrétiser par la publication d'un « **Guide pratique** » accompagné d'une « **check list** » relative aux points à vérifier avant d'entreprendre une migration vers le *cloud*. Tout en informant les clients (publics et privés), cela contribuera à harmoniser les conditions offertes par les fournisseurs.

Enfin en matière de sécurité, l'autorité régulatrice, se fondant sur les recommandations de l'ENISA, devrait mettre en place et faire contrôler un cycle de **rapport** obligatoire des incidents (selon certaines limites ou ordre de gravité), **d'évaluation** des risques qui peuvent en découler et de **mise en place de mesures** pour réduire et annuler ces risques.