CONCOURS EXTERNE DE TECHNICIEN TERRITORIAL - SESSION 2016

Spécialité «INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION»

ÉPREUVE DE QUESTIONS

NOTE OBTENUE : 13.75 / 20

---

1 A. Le Big Data représente un certain nombre d'enjeux pour les collectivités locales. Le stockage et l'utilisation de ces données en interne doit permettre aux collectivités d'améliorer leur fonctionnement en repérant des dysfonctionnements ou repérant des comportements de masse au niveau des utilisateurs de cette collectivité. De même, la mise à disposition de ces données en Open Data peut également être bénéfique pour la collectivité. Elle permet d'une part la mise à disposition des données à tous les citoyens et peut également permettre à des développeurs externes d'utiliser ces données. Ces derniers en créant des applications à partir de ces données permettent d'éviter à la collectivité d'avoir à investir directement dans leur développement.
Si le Big Data est important pour les collectivités, il est aussi source de défis. Le Big Data implique un volume très important de données. Il faut donc, pour les collectivités décider d'un mode de stockage, en interne ou externe, qui dans les deux cas peut avoir un coût important. Se pose également la question de la sécurité de ces données. Bien qu'étant publiques, certaines sont nominatives et ne peuvent être directement utilisées. D'autres peuvent concerner des installations publiques sensibles. La question de la sécurisation de ces données est importante dans le cas de piratage. Il convient également, si il est décidé de passer à l'Open Data de trouver sous quelle licence protéger ces données, ainsi que le format sous lequel elles devront être publiées. Ces différents points impliquent des coûts supplémentaires.

1 B. Le choix d'un logiciel se fera suivant l'utilisation qui en est souhaitée et le budget prévu. Une solution propriétaire représente un investissement premier important mais sera généralement plus accessible en raison de son ergonomie et de ses fonctions abouties. Cependant la non maîtrise du code source de l'application et donc la modification limitée possible en interne peut entrainer des coûts importants de développement en externe. De même, le passage d'une version à une autre du logiciel peut, suivant le contrat initial, entraîner un abandon du logiciel utilisé et la nécessité de devoir tout racheter.
Une solution logicielle libre, elle, demandera un investissement à l'achat moins important. Cependant, pour répondre aux besoins, de nombreux paramétrages et développements complémentaires peuvent être nécessaires, impliquant d'avoir des développeurs en interne et de faire appel à un prestataire. L'utilisateur étant "propriétaire" du code, toute modification du code qu'il voudra y apporter sera possible. L'évolution dans le temps du logiciel est donc responsabilité de l'utilisateur.

2 A. Le BYOD (Bring Your Own Device) consiste à utiliser du matériel informatique personnel dans le cadre d'activités professionnelles, que ce soit ordinateur personnel, tablette ou smartphone. Ce principe peut être voulu par l'entreprise (qui réduit ainsi ses coûts en matériel) ou par l'employé (connexion d'un smartphone sur le WiFi de l'entreprise).
Dans les deux cas, cela pose des problèmes de sécurité et de séparation de la vie professionnelle et privée. En connectant un matériel personnel sur le réseau d'une entreprise, le risque de contamination par un virus ou logiciel espion est accru. La DSI ne connaissant pas l'usage qui a été fait personnellement par l'individu, prend des risques à laisser se connecter un logiciel extérieur. De même, l'entreprise ne peut pas vérifier chaque terminal sous peine d'intrusion dans la vie personnelle. A l'inverse des problèmes peuvent se poser lorsqu'un salarié a, sur son équipement personnel, des données appartenant à l'entreprise.
Il convient donc, à la fois de mettre en place une politique au sein de l'entreprise ou de la collectivité réglementant ces accès, ainsi qu'une politique de sécurité à mettre en place.

2 B. Pour assurer la sécurité d'un SI face à la montée du BYOD, plusieurs mesures complémentaires peuvent être mises en œuvre.
D'une part il convient de sensibiliser les utilisateurs sur les risques encourus pour le SI et pour eux-mêmes dans ce cadre, et de réglementer l'usage du BOYD au sein du SI. Cependant cette mesure est insuffisante. La mise en place d'une sécurité accrue au sein du réseau est nécessaire. De même, il convient de séparer sur chaque terminal l'utilisation personnelle de l'utilisation professionnelle. Des outils de mobile device management permettent, par exemple de chiffrer les données professionnelles sur un terminal et d'en permettre l'accès à partir d'un code.

3 A. Le cloud computing consiste en la mise à disposition par un prestataire d'un ensemble de ressources (logicielles de stockage) et ce à travers Internet. Le prestataires assure la maintenance et le support de ces ressources. On identifie trois grands types de services :

- Le Saas le prestataire fournit ici l'ensemble des services possibles. Il fournit à la fois les serveurs, le stockage et l'application ou les applications nécessaires au client qui n'a pas à s'inquiéter de leur bon fonctionnement
- Le PaaS Le prestataire fournit l'accès au client à des serveurs équipés d'OS et fonctionnels. Le client peut donc y ajouter ses briques logicielles
- Dans le dernier cas, l'IaaS fournit l'accès à un serveur "vierge" qu'il convient au client d'exploiter.

3 B. Il existe deux grands types d'hébergement dan le cadre du Cloud Computing, le public et le privé. Tous deux présentent des avantages et des inconvénients à prendre en compte.

Le Cloud public consiste à partager une certaine puissance de calcul et de stockage avec plusieurs autres acteurs. Cette mutualisation permet une réduction des coûts et dans la théorie une utilisation illimitée des capacités. Cette utilisation est à relativiser : si chaque client exploite grandement les serveurs, les performances peuvent s'en ressentir. De même, l'emplacement des serveurs de données est non connu, ceux-ci peuvent être éclatés dans différents centres. De même, le client ne pourra pas avoir d'exigence précise en termes de sécurité ; l'offre étant mutualisée la sécurité est la même pour tous les clients.

A l'opposé un cloud privé permet plus de souplesse dans le contrat. La sécurité peut être décidée avec le prestataire, tout comme la localisation des données. Le client décide également de la puissance, du stockage nécessaire pour ses ressources. Il n'est plus dépendant de l'activité des autres clients. Ce choix de cloud, plus souple niveau client implique souvent un coût plus élevé.

4. La mise en ligne de données publiques implique de prendre en compte un certain nombre d'aspects juridiques et techniques.

Sur le terrain juridique, il convient de vérifier la nature des informations que l'on souhaite mettre en ligne. Il est ainsi interdit de mettre en accès libre des données nominatives et liées à la vie privée. De même certaines données sensibles peuvent être considérées comme publiques : il convient de faire une analyse juridique préalable pour décider de la pertinence de la publication. Il est également important de choisir une licence pour la publication des données. Cette licence permet de restreindre ou non l'usage qui peut être faite de ces données et leur exploitation.

Sur le plan technique deux points importants sont à relever : le stockage des données, et le format sous lequel elles doivent être publiées. L'Open Data implique un nombre de données toujours croissant et qui peut donc devenir très volumineux. De même, la puissance de calcul peut être mise à mal par un nombre de requêtes trop important. Le choix du format de publication des données est aussi important. Le format permettra une utilisation plus ou moins directe des données et donc un intérêt plus ou moins important selon les cas. certaines informations n'ont de l'intérêt que dans l'immédiat, alors que d'autres prennent une importance dans la durée