Cloud Computing

Quels risques juridiques pour les banques ?

SABINE MARCELLIN
Juriste
Crédit Agricole Corporate and Investment Bank

Codirecteur de la rédaction Guide Lamy Droit de l'informatique et des réseaux

Si le *Cloud Computing*[1] n'est pas une nouvelle technologie, c'est une nouvelle manière de proposer les ressources informatiques aux utilisateurs. Il s'agit de prestations informatiques accessibles sur Internet, qui peuvent aller de l'utilisation d'un logiciel jusqu'à l'externalisation de pans entiers de l'infrastructure informatique. Les services de *Cloud Computing* sont accessibles en ligne et à la demande. Cette apparente facilité explique le rapide développement de cette pratique. Mais la concentration supposée de ressources et données ainsi que la perte potentielle de contrôle des systèmes d'information génèrent également de nouveaux risques, essentiellement en matière de sécurité. Quels sont ces risques du point de vue juridique[2] ? Comment les banques peuvent-elles jouir des bénéfices du *Cloud Computing* sans mettre en danger leur organisation ?

Le *Cloud Computing* n'est pas seulement un concept *marketing* relativement récent et séduisant, il s'agit d'une réalité économique. Cette offre d'accès global aux ressources informatiques permet aux entreprises d'accéder à de nombreux services en ligne, de manière évolutive et en s'exonérant de la gestion de leurs serveurs informatiques. Les applications et les données ne se trouvent plus sur les ordinateurs locaux mais dans un nuage, « *cloud* » en anglais. Le nuage est réparti sur un ou plusieurs centre(s) de traitement ou de stockage[3], comportant un certain nombre de serveurs distants, situés éventuellement dans ou plusieurs pays étrangers, centres interconnectés au moyen d'une large bande passante indispensable à la fluidité du système. L'accès aux services se fait par une application standard facilement disponible, la plupart du temps un navigateur Internet. Les services de *Cloud* sont multiples et les catégories majeures[4] recouvrent notamment l'ingénierie informatique, les infrastructures Internet, la messagerie, la voix sur IP[5], le stockage et l'archivage de données, l'utilisation de logiciels, l'infrastructure et l'assistance informatiques.

Comme les tarifs peuvent paraître attractifs, en particulier en période de rationalisation budgétaire, les utilisateurs sont tentés d'avoir recours à une ou plusieurs prestations « dans le nuage ». Le volume mondial de services de *Cloud Computing* a été estimé en 2009, selon IDC, à 17.4 milliards de dollars et son évolution pour l'année 2013 avoisinerait les 44 milliards. Le marché européen a été estimé à 971 millions d'euros, selon la même source, et devrait s'élever à 6 milliards environ en 2013. Le marché du *Cloud Computing* n'est pas encore mature[6] mais la tendance semble irrésistible.

Quelques précisions techniques peuvent s'avérer utiles pour appréhender le vocable technologique (voir Tableau)

1. Terme anglo-saxon couramment utilisé en français, traduit parfois par « informatique dans le nuage » ou « informatique en nuage ». L'origine de cette expression serait la représentation graphique d'un nuage, métaphore d'Internet dans les schémas d'organisation des réseaux informatiques.
2. Les propos développés dans cet article correspondent à l'approche personnelle de l'auteur et ne sauraient représenter l'opinion de l'entreprise, ni du groupe au sein desquels elle exerce.
3. Souvent désigné par l'expression « Data Center ».
4. IDC Cloud Computing 2010, An IDC Update, sept. 2010.
5. Technique qui permet de communiquer par la voix via Internet.
6. *The What, Why and When of Cloud Computing*, Gartner, June 2009.

et l'organisation de l'informatique en nuage. Les prestations de *Cloud Computing*, accessibles par l'intermédiaire du réseau Internet sont multiples. Elles peuvent comprendre la fourniture de services logiciels (ou « SaaS »), la mise à disposition de plateformes technologiques (ou « Paas ») et des infrastructures d'hébergement (ou « Iaas »). Quant à son architecture, le *Cloud* peut être public ou privé. Le « *Cloud* public » signifie l'hébergement d'applications sur une plateforme dont l'accès se fait uniquement par Internet, c'est-à-dire que cet environnement est, de ce fait, partagé avec un nombre virtuellement illimité d'utilisateurs, qui sont essentiellement les particuliers, pour les messageries personnelles ou le stockage de photos, par exemple, et les petites entreprises. Le « *Cloud* privé » se définit comme une transformation de l'infrastructure interne au moyen de technologies de virtualisation et d'automatisation afin de délivrer, plus simplement et plus rapidement, des ressources informatiques sous forme de services à la demande. Ce mode privé pourrait être davantage adapté aux exigences des grandes entreprises et notamment des établissements bancaires.

Même si le *Cloud Computing* s'appuie sur des technologies classiques, au-delà d'une apparente simplicité d'accès, sa construction globale peut entraîner des vulnérabilités occultées par la complexité technique. Le frein majeur au développement du *Cloud Computing* pour les utilisateurs professionnels, est justifié par le besoin de sécurité, et notamment de confidentialité, et la nécessaire continuité d'activité.

I. LES BÉNÉFICES ET LIMITES DU *CLOUD COMPUTING*

Le développement du *Cloud Computing* semble irréversible. Les avantages affichés par les prestataires sont multiples. Les entreprises peuvent accéder à des services dans des délais plus rapides que ceux offerts par les prestations traditionnelles. Elles peuvent espérer également bénéficier des applications logicielles dans leur version optimale, grâce à une évolution permanente. Elles pourraient ainsi gagner en agilité, c'est-à-dire bénéficier d'une souplesse d'utilisation supérieure à celle de leur infrastructure traditionnelle.

Les bénéfices peuvent aussi se mesurer en termes financiers. En première approche, les investissements en matériels et logiciels informatiques sont fortement réduits. Les coûts des prestations sont variables, à la hausse ou à la baisse, en fonction des besoins des entreprises utilisatrices, en termes d'applications et de volumes de stockage, selon la demande de l'utilisateur.

Les limites du *Cloud Computing* sont à connaître également, avant d'être en mesure de confier tout ou partie de son système d'information à un tiers. De nombreuses applications logicielles standard sont accessibles aujourd'hui sur le *Cloud*, y compris dans le domaine bancaire, même si ce n'est pas le cas pour la majorité des applications. Une autre problématique porte sur la compatibilité des applications externalisées dans le nuage, avec celles qui ne le seraient pas, ou de l'interopérabilité des systèmes gérés par des prestataires de *Cloud Computing* différents. Du point de vue financier, le coût des prestations disponibles en nuage peut être attractif à première vue, mais l'établissement doit mesurer par ailleurs le coût réel à moyen terme, en intégrant le coût du risque. Une autre difficulté liée au *Cloud Computing* est la nécessaire adaptation des méthodes de travail et des procédures de l'établissement, avant qu'il soit en mesure de confier tout ou partie de son système d'information à un tiers.

Mais la question majeure qui retient de nombreuses entreprises, et notamment les banques, est la sécurité du système d'information. Le *Cloud Computing* peut offrir des avantages en termes de sécurité mais soulève des nouvelles problématiques.

II. LA SÉCURITÉ DE L'INFORMATION

Comme dans tous les projets informatiques, la sécurité se mesure en termes de disponibilité d'intégrité et de confidentialité des données, ainsi que de gestion des traces informatiques et preuves. Les risques liés à l'externalisation d'un système d'information sont notamment la qualité de services inadaptée, une insuffisante capacité d'intégration de la part des fournisseurs et leur potentielle défaillance économique ou disparition. Naturellement, les risques existants dans l'informatique traditionnelle sont toujours présents (fraude, catastrophes naturelles, etc.). Cependant, à la différence d'une externalisation traditionnelle, en matière de *Cloud Computing*, certains risques peuvent être favorisés par la concentration des systèmes et leur localisation, notamment les risques d'atteinte à la confidentialité des données.

Le *Cloud Computing* donne l'opportunité de mesurer les effets positifs autant que négatifs en matière de sécurité des systèmes d'information. Comme il est plus rentable d'appliquer des mesures de sécurité à grande échelle, le recours à l'informatique en nuage peut être un facilitateur de sécurité. Les principaux atouts sécuritaires potentiels du *Cloud* sont les suivants :

– multiplicité des lieux de stockage ;

– gestion centralisée des mesures de sécurité et des incidents ;

– gestion centralisée des incidents ;

– centralisation des audits de sécurité et de l'archivage des traces informatiques.

La sécurité du système d'information devient un argument majeur de *marketing* pour les prestataires de *Cloud Computing* mais il semble important de vérifier la réalité derrière le discours. Il est vraisemblable que les opérateurs de *Cloud* seront attentifs aux exigences des utilisateurs et à leurs obligations réglementaires, s'ils souhaitent offrir des prestations adaptées aux systèmes d'information.

Quels sont les risques générés par le *Cloud Computing*, en matière de sécurité du système d'information ? Les risques liés aux projets de *Cloud Computing* ont fait l'objet d'une étude en 2009 par l'ENISA (European Network and Information Security Agency), suivie par la publication d'un rapport en novembre 2009[7]. Dans le cadre de

7. *Cloud Computing. Benefits, risks and recommendations for information security*, nov. 2009.

l'étude, l'ENISA a effectué une analyse de risques, à partir de trois scénarios de *Cloud Computing*, en mettant l'accent sur les besoins des clients de l'entreprise. Le rapport a identifié un ensemble de 35 risques (voir Tableau) susceptibles d'être encourus par les systèmes d'information. Citons quelques risques issus de ce recensement :

– inexécutions liées au réseau, aux systèmes et aux applications ;
– risques de fraude et accès non autorisés aux locaux ;
– application de règles juridiques extra-territoriales ;
– demandes d'accès aux documents par des autorités administratives et judiciaires étrangères ;
– risques liés aux données à caractère personnel ;
– risques liés à la propriété intellectuelle ;
– rupture de la confidentialité ;
– perte ou dégradation de traces (opérationnelles ou de sécurité) ;
– perte de sauvegardes ;
– catastrophes naturelles.

Tous les risques identifiés en matière de *Cloud Computing*, même les risques techniques, peuvent être analysés du point de vue juridique, parce que la responsabilité des acteurs peut être mise en cause, quand les risques se réalisent. Si chaque risque[8] peut revêtir différentes dimensions notamment financière, réputationnelle, commerciale et juridique, la notion de risque juridique[9], en tant que telle, est apparue à une époque récente. Le risque juridique recouvre trois types de vulnérabilités[10] pour l'établissement : le dommage objectif, le comportement transgressif, intentionnel ou non, qui peut générer une action en responsabilité pour faute, et les effets de l'évolutivité de la norme juridique. Selon cette approche, quels sont les risques juridiques associés au *Cloud Computing* ?

III. LES RISQUES JURIDIQUES

Parce que le *Cloud Computing* pourrait être envisagé pour externaliser certaines applications de la banque, et que l'interruption de services sensibles aurait des conséquences difficiles voire désastreuses pour l'activité, les risques doivent être analysés d'un point de vue juridique.

Les risques juridiques majeurs[11] sont les suivants : l'application de règles extraterritoriales, les demandes d'accès aux documents par des autorités administratives et judiciaires étrangères, les risques liés au traitement des données à caractère personnel et les risques liés à la propriété intellectuelle. Comment appréhender ces différents risques juridiques dans le cadre d'une externalisation vers le *Cloud Computing* ?

1. L'application de règles extraterritoriales

L'application de règles extraterritoriales peut être perçue comme un risque, car la localisation des données pourra déterminer le droit applicable au patrimoine informationnel de l'entreprise. Comme par nature les données hébergées dans le *Cloud*, peuvent être transférées dans un pays ou un autre, en fonction des choix techniques du prestataire, cette localisation revêt une grande importance pour l'établissement client. Si la banque a une activité en France, naturellement les autorités administratives et judiciaires peuvent accéder à certains documents, selon certaines procédures[12] connues par la banque. Les procédures émanant des autorités françaises ne sont pas perçues comme un risque pour le système d'information. Il n'en est pas de même pour les autorités étrangères, car ces procédures peuvent être différentes, méconnues ou en contradiction avec les procédures nationales.

2. Les demandes d'accès aux documents par des autorités administratives et judiciaires étrangères

Une autre question sensible pour le *Cloud Computing* est générée par la localisation des données. Suivant le lieu de stockage du corpus informationnel, le droit applicable pourra varier. Les données pourront ainsi faire l'objet de demandes par des autorités administratives et judiciaires étrangères, émanant potentiellement d'un grand nombre de pays différents. Certains pays peuvent s'avérer plus risqués que d'autres, pour différentes raisons : régimes autocratiques, non-respect des conventions internationales, etc.

Les États disposant de systèmes juridiques avancés peuvent également présenter des menaces. Dès lors que les serveurs de *Cloud* se trouvent dans certains pays de « Common law », les entreprises françaises peuvent être sollicitées pour produire des documents électroniques dans ces pays. Par exemple, les procédures judiciaires de *pre-trial discovery*[13] américain ou de *disclosure*[14] en Grande-Bretagne requièrent qu'une entreprise communique à la partie adverse tous les éléments de preuve dont elle dispose au cours de l'instruction d'une affaire. Ces mesures judiciaires ne sont pas critiquables a priori, mais leurs conséquences peuvent représenter des risques pour l'entreprise française, notamment parce que la réglementation française peut s'opposer à cette communication : secret bancaire, loi de blocage, etc. La loi dite « de blocage »[15], par exemple, sous réserve des traités et accords internationaux, interdit la communication de documents et renseignements d'ordre économique, commercial, financier ou technique, à des personnes physiques ou morales étrangères. Ce texte s'applique dès lors que cette communication est de nature à constituer une menace notamment à l'égard des intérêts économiques essentiels de la France, ou qu'elle tend à la constitution de preuve dans le cadre d'une procédure judiciaire ou administrative étrangère.

8. *Combinaison de la probabilité d'un événement et de ses conséquences*, guide ISO/IEC Guide 73.2002, AFNOR.
9. Jacques Dupichot, « Regards sur le nouveau juriste d'entreprise et la gestion du risque juridique », in *Aspects du droit privé en fin du XX^e siècle, Études réunies en l'honneur de Michel de Juglart*, LGDJ, 1986. Hervé Bidaud, Patrick Bignon et Jean-Paul Cailloux, La Fonction juridique et l'entreprise, Eska, 1995.
10. Franck Verdun, *La Gestion des risques juridiques*, Éd. Organisation, 2006.
11. Selon l'étude de l'ENISA précitée.
12. Voir Sabine Marcellin, « La dimension juridique de l'archivage électronique », *Banque & Droit* n° 133, sept.-oct. 2010.
13. *Federal Rules of Civil Evidence, Amendments*, 1^er déc. 2006.
14. *Civil Procedures Rules*, SI 1998/3132.
15. Loi n° 68-678 du 26 juill. 1968.

Des dispositions légales autorisent la communication d'informations à des autorités publiques étrangères, fondées sur la mise en place de systèmes de coopération entre autorités de supervision publique. Dans le domaine bancaire, l'Autorité de Contrôle Prudentiel française a passé différents accords avec des autorités de contrôle de pays tiers. Pour la coopération judiciaire, la convention de La Haye du 18 mars 1970 sur l'obtention de preuve à l'étranger et le Règlement[16] du Conseil du 28 mai 2001 relatif à la coopération entre les juridictions des États membres dans le domaine de l'obtention des preuves en matière civile ou commerciale, déterminent les procédures de communication des pièces en vue d'une utilisation dans un procès à l'étranger.

Afin de s'assurer que l'accès aux documents par une autorité étrangère, dans le cadre de procédures judiciaires ou administratives, n'est pas contradictoire avec des exigences réglementaires ou contractuelles, l'établissement devra disposer d'un avis juridique pour mesurer les différents risques et déterminer, en toute connaissance de cause, la position à tenir.

Certains prestataires de *Cloud*, conscients de la problématique, proposent des offres dans laquelle la prestation est circonscrite à une zone géographique déterminée.

3. Les risques liés au traitement des données à caractère personnel

Les dispositions de la loi Informatique et Libertés[17] imposent à l'établissement un ensemble d'obligations relatives au traitement des données à caractère personnel, et notamment des formalités déclaratives, des astreintes en matière de collecte, de durée de conservation et de sécurité des données. Toutes ces obligations s'appliqueront dans le cadre du *Cloud Computing*.

Parmi celles-ci, l'article 34 de ladite loi impose un devoir général de sécurisation des données à caractère personnel : « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.* ». L'entreprise reste responsable, même en cas d'externalisation de son activité, selon l'article 35 : « *Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.* »

La banque responsable du traitement est tenue de mettre en œuvre des mesures de sécurité, proportionnées à la nature des données. Ainsi l'obligation de sécurité sera renforcée si les données sont sensibles (données relatives à la santé, par exemple). Le non-respect de cette obligation peut entraîner des sanctions : une sanction administrative[18] prononcée par la CNIL (Commission nationale de l'informatique et des libertés) ou une sanction pénale[19]. Si les opérations de *Cloud Computing* entraînent un transfert de données hors de l'Union européenne, l'établissement devra porter une attention spéciale aux dispositions particulières[20] de la loi Informatique et Libertés en matière de transfert de données à caractère personnel vers l'étranger.

De plus, les instances européennes réfléchissent actuellement, sous l'angle de la protection des consommateurs, à la mise en place d'un cadre harmonisé de protection de la vie privée. Cette évolution imposerait à toute entreprise d'informer, de toute violation de sécurité des données, le régulateur en charge de la protection des données[21] et toutes les personnes physiques qui seraient concernées par la violation de sécurité de leurs données.

Il semble difficile pour le client de *Cloud Computing* de vérifier effectivement comment est assurée la protection des données. Le client ne peut effectuer directement de vérification, mais seulement par le biais de contrôles et audits, organisés dans le cadre du contrat. Ce risque revêt une acuité particulière pour le traitement des données à caractère personnel car le client devra s'assurer que ce traitement est conforme à la réglementation applicable en la matière. Il est évident que le responsable des données à caractère personnel, au sens de la loi est bien l'établissement et que le prestataire de *Cloud Computing* est un « sous-traitant », au sens de cette même loi. Ce qui signifie que les inexécutions potentielles pourront mettre en jeu la responsabilité de l'établissement, dans le cadre de procédures administratives ou pénales, et naturellement générer un risque d'atteinte à l'image et la réputation.

Un autre point de vigilance porte sur la durée de conservation et la destruction des documents gérés dans le *Cloud Computing*. Les durées de conservation d'archives bancaires et les délais de prescription restent un thème important à suivre, que les documents soient localisés dans ou hors de l'entreprise. La difficulté nouvelle apportée par le *Cloud Computing* est d'avoir la preuve de la destruction des documents, qui peuvent être dupliqués sur plusieurs sites. La durée de conservation est un sujet sensible, en particulier quand il s'agit de données à caractère personnel, sachant que la réglementation[22] prévoit que cette durée

16. Règlement 1206/2001.
17. Loi n° 78-17 du 6 janv. 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
18. Sanction de 150 000 euros ou, en cas de manquement réitéré, jusqu'à 3 000 000 d'euros, et d'autres sanctions administratives notamment selon l'article 47 de la loi n° 78-17.
19. Amende de 300 000 euros et cinq ans de prison.
20. Consulter le guide publié par la CNIL relatif aux transferts de données à caractère personnel, disponible sur son site Web (www.cnil.fr).
21. La Commission informatique et libertés, en France ou ses homologues européens.
22. Article 6 de la loi n° 78-17 du 6 janv. 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

doit être adaptée à la finalité du traitement de données. Afin de respecter le droit à l'oubli, l'établissement devra s'assurer que les procédures de conservation et de destruction de documents électroniques sont conformes aux exigences légales.

4. Les risques liés à la propriété intellectuelle

La propriété intellectuelle des créations de l'établissement, intégrées dans le système d'information hébergé dans le *Cloud*, représente également une question délicate. Les créations peuvent être de différentes natures : logiciels, éléments protégés par les droits d'auteur par le droit des marques, des brevets, par la protection *intuitu personae* des bases de données ou encore le savoir-faire.

De plus, les droits de propriété intellectuelle des tiers, attachés à des documents éventuellement contenus dans le *Cloud* peuvent soulever quelques difficultés, par exemple un procédé brevetable dont le développement est financé par une banque. Outre l'approche du secret bancaire, qui sera abordée ci-après, les informations confiées par les clients à leur banque peuvent être objets de protection intellectuelle au profit desdits clients.

Par ailleurs il conviendra d'être vigilant quant aux conditions d'utilisation de logiciels, dont sont titulaires des éditeurs tiers et pour lesquels l'établissement bénéficie d'une licence d'utilisation et de vérifier dans quelles conditions, juridiques et techniques, ces logiciels peuvent être confiés au prestataire de *Cloud Computing*.

Même si les règles de protection de la propriété intellectuelle sont harmonisées au sein de l'Union européenne, une atteinte aux droits de propriété intellectuelle pourrait causer un dommage immédiat, qui ne pourrait apporter de réparation, que dans le cadre d'une procédure judiciaire. Les solutions consisteront à examiner l'opportunité de confier ou non à un tiers certaines catégories d'informations. Et naturellement le contrat passé avec le prestataire devra intégrer les droits de propriété intellectuelle et les mesures de sécurité adaptées.

IV. LES EXIGENCES SPÉCIFIQUES DU SYSTÈME D'INFORMATION BANCAIRE

Outre les risques applicables aux entreprises en général, certains risques liés au système d'information prendront un relief particulier du fait de l'activité bancaire et de sa réglementation propre. Sur ce thème, une synthèse des obligations applicables aux banques en matière de sécurité des systèmes d'information devrait être rendue publique prochainement, préparée par le Forum des Compétences[23]. Parmi les obligations majeures des établissements, citons le devoir général de sécurité issue du CRBF 97-02, le secret bancaire, l'accès aux données par les régulateurs bancaires français, les prestations de services essentiels externalisées et les exigences contractuelles dans le domaine de la monétique.

1. Le règlement CRBF 97-02

Le règlement CRBF 97-02[24] impose aux établissements bancaires et financiers une obligation générale de sécurité des systèmes d'information. Notamment, son article 37-2 précise : « Les entreprises assujetties qui externalisent [...] demeurent pleinement responsables du respect de toutes les obligations qui leur incombent. » Les établissements doivent mettre en place, en cas d'externalisation des prestations essentielles, des mécanismes de sécurisation des systèmes d'information, un plan de continuité d'activité et l'élaboration de manuels de procédures. Les obligations devront être étendues à l'offreur de *Cloud Computing* mais, en cas de défaillance, la responsabilité reste celle de l'établissement. Le contrat avec l'opérateur de *Cloud* devra encadrer les obligations des parties.

2. Le secret bancaire

En confiant certaines activités à un opérateur externe au travers du *Cloud Computing*, la banque peut être amenée à communiquer des informations sur ses clients, couvertes par le secret bancaire[25]. Quel que soit le lieu de stockage des données, notamment à l'étranger, la banque doit s'assurer par des moyens techniques, organisationnels et contractuels, que le secret bancaire sera protégé conformément au droit français.

3. L'accès aux données par les régulateurs bancaires français

Quel que soit le lieu de stockage des données, l'établissement financier doit être capable, à tout moment de répondre favorablement à une demande émanant d'un régulateur français ou européen, et en particulier dans le domaine bancaire. L'Autorité de Contrôle Prudentiel peut exiger[26] tous renseignements, documents quel qu'en soit le support et en obtenir copie. De même, l'AMF peut également demander[27] communication de pièces nécessaires à une mission de contrôle ou à une enquête. Les conditions d'hébergement des données concernées permettent-elles un accès exhaustif et dans des conditions conformes aux demandes d'une autorité ? Cet aspect devra être formalisé dans le contrat des relations contractuelles avec l'offreur de *Cloud*.

4. Les prestations de services essentiels externalisées

Les prestations de services essentielles désignent les opérations de banque et toute prestation de services présentant un effet significatif sur la maîtrise des risques. Selon le CRBF 97.02[28], lorsque la réalisation de ces prestations est confiée à un prestataire, les établissements

23. « Les obligations en matière de sécurité des systèmes d'information », Forum des compétences. Cette publication est à paraître sur le site sur le site « forum-des-competences.org ». Le Forum des compétences est une association d'établissements bancaires, de sociétés d'assurance et de régulateurs qui travaillent et échangent sur le thème de la sécurité des systèmes d'information.

24. Règlement n° 97-02 du 21 févr. 1997 modifié relatif au contrôle interne des établissements de crédit et des entreprises d'investissement.

25. Article 511-33 du Code monétaire et financier.

26. Article L. 612-24 du Code monétaire et financier.

27. Article L. 621-9 du Code monétaire et financier ; articles L. 143-2 et L. 144-2 du Règlement Général de l'AMF.

28. Arrêté du 2 juill. 2007 modifiant le règlement 97-02 du Comité de la réglementation bancaire et financière du 21 févr. 1997 relatif au contrôle interne des établissements de crédit et des entreprises d'investissement.

devront conserver l'entière maîtrise des activités externalisées et notamment signer un contrat avec celui-ci. Ils doivent veiller également à ce qu'il s'engage sur un niveau de qualité, mette en œuvre des mécanismes de secours, et rende compte à l'établissement de manière régulière sur la manière dont est exercée l'activité externalisée. Les prestataires devront également accepter que les régulateurs aient accès aux informations sur les activités externalisées, y compris sur place. La conformité à ces dispositions suppose donc une identification par les établissements de leurs prestations essentielles et une formalisation adaptée des contrats passés avec leurs prestataires, notamment de *Cloud Computing*, qui devront intégrer ces exigences de contrôle.

5. Les exigences dans le domaine de la monétique

Une autre obligation de sécurité s'impose aux établissements financiers, dans le domaine de la monétique. La norme PCI DSS[29] n'est pas une obligation réglementaire mais une exigence contractuelle incontournable pour tous les établissements qui proposent des cartes de paiement. L'objectif de cette norme est de renforcer la sécurité des données des titulaires de cartes, dans le cadre de mesures uniformes au niveau international. Ainsi, un certain nombre de conditions spécifiques de sécurité seraient à surveiller particulièrement dans le cadre de prestations en nuage.

V. QUELLES SOLUTIONS ?

Si une banque envisage d'avoir recours au *Cloud Computing* pour l'exploitation d'une partie de son système d'information, elle va procéder à une analyse de risque. Cette analyse représente, comme pour tout projet, une étape essentielle et obligatoire[30], avant de prendre la décision de confier certaines applications à un opérateur. Il s'agit d'identifier les causes possibles d'une défaillance du système d'information, d'en évaluer les conséquences et de mettre en place les mesures de sécurité pour réduire le risque à un niveau acceptable. L'analyse de risque se fonde classiquement, depuis le Livre Blanc sur la sécurité des systèmes d'information dans les établissements de crédit[31], sur l'étude de la sensibilité DICP : Disponibilité, Intégrité, Confidentialité et Preuve.

Cette démarche permettra d'apporter les mesures nécessaires à la sécurité des données externalisées et de faire les choix adaptés.

La banque devra examiner avec une grande attention la localisation des données, car le fait que ces données soient transférées sur un territoire ou un autre aura des effets sur le droit applicable et pourra engendrer des obligations particulières. Certains opérateurs majeurs du *Cloud* semblent avoir conscience de l'implication légale de la localisation de leurs serveurs et proposent le choix quant à la localisation et disposent notamment d'offres localisées au sein de l'Union européenne.

Parmi les moyens d'assurer la confidentialité, le chiffrement des données peut permettre d'assurer la confidentialité. Il sera nécessaire dans ce cas de vérifier, suivant la localisation des données, quelles dispositions légales s'appliquent. Sur le territoire français, l'utilisation du chiffrement est relativement souple[32], c'est-à-dire que l'utilisation est libre mais cependant la fourniture, l'importation et l'exportation de moyens de cryptologie sont contrôlées par des obligations de déclaration ou d'autorisation. Il convient de vérifier si, en fonction de la localisation des serveurs du *Cloud*, quelles sont les dispositions légales qui limiteraient voire interdiraient le chiffrement. L'anonymisation de certaines catégories de données peut également représenter une solution pour renforcer la confidentialité.

En convergence avec les mesures de sécurité organisationnelles et technologiques, le contrat, négocié et signé avec le prestataire, permettra au client de *Cloud Computing* d'obtenir la mise en œuvre de mesures de sécurité et de qualité de services. Le contrat devra être construit, en accord avec l'opérateur, en intégrant les exigences de l'établissement et de ses obligations réglementaires. Les obligations contractuelles présentes dans tout contrat d'externalisation s'appliqueront aux prestations de *Cloud Computing*. Les points majeurs à traiter porteront notamment sur la sécurisation des applications et des données, y compris des données à caractère personnel, la confidentialité et l'organisation d'audits de sécurité. Dans un esprit de prévention des risques juridiques, seront également importantes les clauses relatives à la qualité de service[33], à la localisation des données, à l'avertissement du client en cas de faille de sécurité, aux conditions de restauration de données et la réversibilité, permettant de rapatrier les données ou de les transférer à d'autres prestataires.

Le *Cloud Computing* représente une forme d'évolution des systèmes d'information pouvant apporter des avantages à une entreprise bancaire, ainsi qu'un ensemble de risques. Avant d'être en mesure de confier une application informatique au « nuage », il conviendra de procéder à une solide analyse des risques et de contrôler les vulnérabilités identifiées, dans le cadre de mesures organisationnelles, techniques et naturellement juridiques. ■

29. *Payment Card Industry Data Security Standard* élaborée par les réseaux émetteurs de cartes, dont la version 2.0 est entrée en vigueur le 1er janv. 2011.
30. Article 37-2 du Règlement CRBF 97-02.
31. Livre Blanc élaboré en 1996 par la Commission bancaire et le Forum des compétences.
32. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, décret n° 2007-663 du 2 mai 2007 pour l'application des articles 30, 31 et 36 de la LCEN et relatif aux moyens et aux prestations de cryptologie et décret n° 2001-1192 du 13 déc. 2001 relatif au contrôle de l'exportation, à l'importation et au transfert des biens et technologies à double usage.
33. *Service Level Agreement* ou convention de niveau de service.

POUR EN SAVOIR PLUS

■ ENISA – European Network and Information Security Agency. Benefits, risks and recommendations for information security : http://www.enisa.europa.eu.

■ Forum des Compétences de la sécurité des systèmes d'information : Obligations en matière de sécurité des systèmes d'information (Document publkié en juin 2011 et consultable en ligne : http://www.forum-des-competences.org.

Typologie des risques liés au *Cloud Computing*

(Source ENISA, traduction de l'auteur)

1. Enfermement
2. Perte de contrôle
3. Non-conformité réglementaire
4. Perte d'activité due aux activités de « co-locataires »
5. Cessation de service
6. Acquisition du fournisseur par un tiers
7. Rupture de la chaîne d'approvisionnement
8. Insuffisance des ressources
9. Non-étanchéité des ressources
10. Fraude interne au fournisseur de *Cloud*
11. Défaillance de l'interface de gestion
12. Interception de données en transit
13. Fuites de données sur place
14. Suppression inefficace ou non-sécurisée des données
15. Déni de service
16. Déni de service pour raison économique
17. Perte de clés de chiffrement
18. Accès malveillant aux données
19. Défaillance de l'application centrale du prestataire
20. Conflits entre les procédures des clients et l'environnement du *Cloud*
21. Risques générés par les procédures administratives ou judiciaires
22. Risques générés par l'application de règles extra-territoriales
23. Risques liés à la protection des données à caractère personnel
24. Risque en matière de propriété intellectuelle
25. Défaillance du réseau
26. Utilisation non optimale du réseau
27. Évolution du trafic réseau
28. Gestion défaillante des habilitations d'accès
29. Attaques de type « ingénierie sociale »
30. Perte ou défaillance des traces opérationnelles
31. Perte ou défaillance des traces de sécurité
32. Altération des sauvegardes
33. Accès non autorisé aux locaux
34. Vol du matériel informatique
35. Catastrophes naturelles

La terminologie du *Cloud Computing*

■ ***Cloud Computing*** **:** prestation informatique permettant aux utilisateurs d'accéder à des ressources informatiques (applications, données) par l'intermédiaire d'Internet, ces ressources étant déportées sur un certain nombre de serveurs distants interconnectés entre eux, plutôt que sur les ordinateurs des utilisateurs.

■ ***Saas – Software as a Service*** **:** mise à disposition par Internet d'applications informatiques (logiciels) comme un service, dans le cadre d'un abonnement, les données étant également stockées sur un serveur de l'opérateur.

■ ***PaaS – Platform as a Service*** **:** fourniture d'un environnement de développement et d'exploitation de logiciels sur Internet.

■ ***IaaS – Infrastructure as a Service*** **:** sous cette appellation, on désigne une infrastructure matérielle, louée à la demande (stockage, machines virtuelles, système d'exploitation, etc.). L'utilisateur peut, dans ce cas, disposer sur demande d'une capacité de traitement pour n'importe quel type d'application.