



EN DROIT

Stéphanie Chuffart-Finsterwald
Thomas Goossens,
Avocats, Bianchischwald

Guide «Cloud» Swissbanking: Quelles avancées?

Si l'informatique en nuage – dite «cloud computing» – offre des perspectives intéressantes pour le secteur bancaire suisse, celui-ci avait jusqu'à présent réservé un accueil mitigé à ces technologies, craignant les conséquences légales et réglementaires des incertitudes qui planent sur la pratique. C'est en particulier le cas en ce qui concerne le respect du secret bancaire, l'exercice du droit de contrôle de la FINMA et les obligations relatives à la protection des données personnelles.

En mars dernier, l'Association suisse des banquiers (ASB) a publié son Guide pour les banques et négociants en valeurs mobi-

lières qui recourent ou souhaitent recourir au cloud computing. Le Guide se concentre sur quatre domaines à savoir (i) le choix du prestataire et de ses sous-traitants, (ii) le traitement des données et le secret bancaire, (iii) la transparence et la coopération entre les établissements et les prestataires en ce qui concerne les mesures administratives et judiciaires et (iv) le contrôle des prestations et de l'infrastructure (audit). Le Guide établit des bonnes pratiques non contraignantes en la matière. Bien que ces recommandations ne répondent pas à toutes les questions pratiques – elles n'ont d'ailleurs pas vocation à le faire, elles offrent des éclaircissements bienvenus sur quelques aspects clés.

En premier lieu, le Guide souligne l'utilité et les avantages du cloud computing pour le secteur bancaire, vantant les économies de coûts que ces prestations de services permettent, ainsi que les possibilités d'offre de produits innovants et d'amélioration de la sécurité de l'infrastructure bancaire, cela en particulier pour les établissements de petite taille. Le recours au cloud computing par le secteur bancaire suisse est ainsi non seulement validé mais également encouragé par l'ASB.

Ensuite, le Guide formule des recommandations intéressantes en ce qui concerne le traitement des données et le secret bancaire. En particulier, il établit que dès lors que l'établissement a prévu des mesures de sécurité appropriées pour protéger les Client Identifying Data (CID) traitées, il n'a pas besoin d'être délié du secret bancaire par le client. L'établissement doit à ce titre avoir pris des mesures techniques (anonymisation, pseudonymisation ou cryptage), organisationnelles (surveillance et audit obligatoire) et contractuelles limitant le risque que le prestataire et les sous-traitants accèdent aux CID. Les mesures à mettre en œuvre résultent de l'annexe 3 de la Circulaire FINMA sur les risques opérationnels (08/21). Le Guide rappelle toutefois que selon le modèle de service dans lequel s'inscrit le cloud computing, il peut être nécessaire que des collaborateurs du prestataire et de ses sous-traitants aient accès aux CID sans cryptage ni pseudonymisation. Selon le Guide, les prestataires et sous-traitants peuvent alors être qualifiés de mandataires au sens de l'art. 47 al. 1 LB et peuvent ainsi être inclus dans le cercle des personnes tenues au secret, même s'ils sont domiciliés à l'étranger. A ce titre, il sied de rappeler qu'en tout état, la loi sur la protection des données conditionne le transfert de données

personnelles (par exemple des CID) à une partie sise dans un Etat ne garantissant pas un niveau de protection adéquat à certains prérequis comme le consentement éclairé (voire exprès) de la personne concernée. Il convient également de souligner, même si le Guide n'en fait pratiquement pas état, que les exigences de la Circulaire FINMA Outsourcing (18/3) demeurent applicables à toute externalisation d'une fonction essentielle par une banque. Sur ce point, on se souviendra que la FINMA elle-même considèrerait l'activité de «stockage de données» comme étant soumise aux exigences en matière d'outsourcing bancaire, du moins sous l'égide de l'ancienne Circulaire 08/7.

En ce qui concerne l'audit des prestataires, le Guide prescrit des contrôles réguliers. Il rappelle que des contrôles doivent pouvoir être réalisés par les établissements, leurs sociétés d'audit ainsi que par la FINMA et indique que des audits groupés peuvent être organisés, ce qui peut encourager une coordination du secteur bancaire sur ce point.

Le Guide formule finalement des recommandations en ce qui concerne la collaboration des prestataires avec des autorités en cas de demande ayant pour objet la transmission d'informations protégées par le secret bancaire et indique en particulier que pour ces cas les établissements doivent convenir d'une marche à suivre qui assurera le respect des prescriptions légales en la matière. Comme pour la majorité de ses recommandations, le Guide fait fi de l'inégalité existante entre les différents établissements bancaires quant à leur faculté de négocier des clauses contractuelles spécifiques face aux poids lourds de l'industrie du cloud computing. Affaire à suivre donc... ■