Outsourcing et traitement des données électroniques des clients

Me MARCO VILLA
Associé- FBT Avocats

La diminution de la rentabilité des établissements bancaires découlant d'un cadre législatif et réglementaire ainsi que d'un environnement international de plus en plus contraignants crée une pression sur les coûts d'exploitation.

Les banques sont à la recherche constante de solutions permettant de maîtriser ces coûts. L'externalisation de certaines activités est une option souvent envisagée. Mais toute délégation à des tiers présente un risque pour l'établissement qui délègue. La FINMA a posé certains principes en matière de délégation et va prochainement mettre en œuvre de nouvelles règles relatives à l'outsourcing du traitement des données électroniques de clients.

Avec l'augmentation de la transparence, notamment sous l'angle fiscal international, et le démantèlement progressif des règles en matière de secret bancaire, les établissements bancaires ont peu à peu perdu l'avantage concurrentiel (quasi protectionniste) lié au secret bancaire, avec pour conséquence l'érosion de leurs marges. Dans ce contexte, l'externalisation de certaines activités auprès de prestataires tiers peut représenter une intéressante économie de coûts. C'est en particulier le cas dans le domaine du traitement des données électroniques, où les frais associés à la création, à la maintenance et au développement régulier d'une infrastructure informatique performante sont souvent colossaux. Si l'outil informatique est absolument nécessaire à l'exécution des tâches de la banque (que ce soit pour le suivi des comptes, la tenue de la comptabilité ou encore le reporting), il est souvent grand consommateur de personnel qualifié (informaticiens, chefs systèmes, administrateurs de données, etc.). Il nécessite un soin constant, doit être maintenu en état de fonctionnement permanent, être adapté à l'évolution de l'environnement technologique et aux demandes de la clientèle (e-banking, prestations mobiles, etc.) et présenter toutes les garanties de sécurité en termes de protection des données.

L'externalisation par les banques de leurs activités est régie par la Circulaire FINMA 2008/7 relative à l'outsourcing bancaire, qui pose les principes réglementaires à une telle délégation lorsque les activités déléguées sont considérées comme *«essentielles»*. Tel est le cas lorsque les activités concernées peuvent avoir un impact sur la détermination, la limitation et le contrôle de divers risques non seulement financiers, mais également juridiques, de réputation et opérationnels. La circulaire fixe les conditions auxquelles l'outsourcing est soumis. Ainsi, un contrat écrit doit – sauf exception – régir les rapports entre l'entreprise délégante et le prestataire auquel une tâche est confiée. Ce contrat doit notamment définir les niveaux de prestations attendus et rendre l'évaluation de la performance possible, sous l'angle qualitatif et quantitatif. Le délégataire doit être soigneusement choisi, instruit et contrôlé ; ses compétences doivent être déterminées et délimitées avec précision. Le délégant et le délégataire doivent enfin fixer les exigences en matière de sécurité et élaborer les dispositifs idoines. Les données, plus particulièrement celles des clients (notamment électroniques), doivent être protégées au moyen de mesures organisationnelles et techniques appropriées pour prévenir tout traitement non autorisé. Les mesures mises en place doivent garantir que les données ne seront pas détruites de façon accidentelle ou non autorisée, perdues, affectées d'erreurs, falsifiées, volées, copiées, utilisées ou modifiées sans droit, ou encore rendues accessibles à des tiers non autorisés. Par ailleurs, ces mesures doivent faire l'objet d'un réexamen périodique: l'évolution de la technique, de l'environnement et des menaces justifient que les mesures de protection prises soient réévaluées et, le cas échéant, adaptées sur une base régulière, voire immédiatement à la suite d'un incident.

LA FINMA VEUT DE L'INDÉPENDANCE

Lorsque de surcroît, des données concernant des clients sont transférées à l'étranger à l'occasion d'une opération d'externalisation, l'établissement bancaire déléguant doit s'assurer que leur protection sera garantie à l'étranger également, de manière conforme au droit suisse. Les exigences qui précèdent font l'objet d'un important développement dans le cadre de la Circulaire FINMA 2008/21, consacrée aux «*exigences de fonds propres et exigences qualitatives relatives aux risques opérationnels dans le secteur bancaire*», complétée par une nouvelle annexe relative au *«Traitement des données électroniques de clients»* (Annexe n° 3) dont l'entrée en vigueur est prévue au 1er janvier 2015. Les récentes (et désagréables) expériences de certains établissements bancaires en Suisse et à l'étranger (vol de CD contenant des données de clients, piratage externe de bases de données bancaires, etc.) ont convaincu la FINMA du fait que le traitement de données électroniques relatives à la clientèle d'une banque représente un risque opérationnel majeur, pouvant avoir des conséquences graves aussi bien sur le plan économique qu'en terme de réputation pour l'établissement. C'est a fortiori le cas lorsque le traitement des données fait l'objet d'une externalisation qui peut de surcroît impliquer un transfert de ces données vers l'étranger. La FINMA pose ainsi dans la nouvelle Annexe n°3 à ▶▶

sa Circulaire 2008/21 un certain nombre de principes relatifs à la bonne gestion du risque lié au traitement de données électroniques relatives à la clientèle.

La FINMA impose désormais à tous les établissements bancaires la création d'une *«unité indépendante»,* qui agit sous la supervision de la direction générale, et dont la mission est l'établissement, la préservation et le contrôle du respect des conditions-cadres devant garantir la confidentialité des données des clients. Cette unité doit être indépendante des unités en charge des traitements de données. Les banques doivent par ailleurs élaborer et documenter par écrit un concept-cadre relatif à la confidentialité des données, identifiant les risques y relatifs et fixant de façon complète les activités, processus et systèmes garantissant la confidentialité. Ce concept-cadre doit tenir compte d'une classification des données traitées selon leur nature (données dites *«d'identification directe»* comme le nom, le prénom, etc., celles dites *«d'identification indirecte»* comme un numéro de passeport, ou encore celles dites *«d'identification potentiellement indirecte»* comme celles résultant d'un recoupement d'une date de naissance avec une profession et une adresse, etc.) et prévoir la mise en œuvre de mesures de protection (données brutes, chiffrement, pseudonymisation, anonymisation) selon le niveau de confidentialité requis et le traitement qui en est fait.

Sont également prévues des règles concernant la sécurité des lieux de stockage et l'accès aux données (tenue d'une liste des applications et infrastructures qui renferment des données, lieux de stockage sécurisés, autorisations d'accès aux données et aux lieux de stockage sur une base *«need to know»*, etc.). Elles rappellent que le stockage hors de Suisse ou l'accès aux données depuis l'étranger impliquent des risques accrus qui doivent être atténués de façon appropriée, les établissements devant, le cas échéant, prévoir des mesures de sécurité plus importantes. Les infrastructures et la technologie utilisées pour le stockage et le traitement des données doivent permettre notamment de garantir la sécurité des données non seulement au point terminal de leur utilisation (ordinateur de bureau, ordinateur portable, appareil mobile, etc.), mais également durant leur transfert depuis leur point de stockage (sécurité du réseau utilisé, notamment si les données sont réparties sur plusieurs sites), et bien sûr au lieu de stockage. Les établissements bancaires sont tenus de suivre l'évolution de la technique et d'adapter régulièrement leurs solutions de sécurité aux pratiques du marché. Le facteur humain doit également être pris en compte : les collaborateurs doivent être soigneusement choisis et leur niveau d'accréditation en ce qui concerne l'accès aux données évalué également sous l'angle d'un risque pour leur confidentialité. Les personnes ayant accès à un grand nombre de données (par exemple les informaticiens) doivent répondre à des exigences supérieures de sécurité.

TOUJOURS PLUS DE PROTECTION

Enfin, en cas d'externalisation d'activités et des prestations de services en relation avec le traitement de données de clients, la capacité du délégataire à garantir cette confidentialité est un élément essentiel dans le choix du délégataire. Lorsque l'externalisation concerne des prestations de services en relation avec de grandes quantités de données relatives à la clientèle, des critères d'évaluation fixant les standards attendus en matière de confidentialité et de sécurité doivent être fixés par le délégant ; ce n'est que si le prestataire envisagé répond à ces critères qu'il peut être sélectionné, étant précisé que cette évaluation doit intervenir avant chaque nouveau contrat, même s'il s'agit d'un prestataire précédemment agréé. Le contrat avec le tiers prestataire doit prévoir qu'il se conformera aux standards de confidentialité et de sécurité établis par l'établissement bancaire, tels qu'ils résultent du concept-cadre qui aura été communiqué au prestataire.

La FINMA prend très au sérieux la question de la sécurité et de la confidentialité des données électroniques, en particulier lorsque celles-ci font l'objet d'un traitement externalisé. Avec raison. Les technologies modernes permettent des traitements de données à très grande échelle et à très grande vitesse ; un défaut de sécurité ou une rupture de confidentialité, en particulier lorsqu'un grand nombre de données sont concernées, peut avoir de graves et rapides conséquences sur le fonctionnement de la banque. Le risque est évidemment plus grand encore lorsque le traitement des données est externalisé. Dans un monde où les banques comme leurs clients souhaitent pouvoir accéder à des données de façon presque universelle, notamment par le biais d'outils de communication mobiles, et que l'outsourcing apparaît comme une solution séduisante, voire nécessaire, les besoins de protection – et les coûts d'implémentation qui en découlent – vont continuer à s'accroître, avec pour curieuse conséquence un besoin accru d'outsourcing. ■ **MV**