Pour protéger des données très recherchées

Les récentes affaires ayant bousculé le secret bancaire suisse requièrent une refonte du système et à l'adoption de nouvelles bonnes pratiques.

NICOLAS CAPT, ALEXIS PFEFFERLÉ, avocats, associés fondateurs d'Heptagone digital risk management & security*

Il y a quelques semaines, Le Monde révélait les détails de l'«Opération Chocolat», nom de code donné au recrutement par les services fiscaux français, à Genève, de l'informaticien de HSBC, Hervé Falciani, et l'exploitation mondiale des données bancaires qu'il avait dérobées en 2008. Quelques jours plus tard, c'est un média suisse qui brossait un portrait sans équivoque du plus célèbre lanceur d'alerte du pays, dont on apprenait qu'il était au fond aussi manipulateur que manipulé. L'affaire Falciani, au-delà du scandale fiscal qui l'a nourrie, de la traîtrise d'un homme et de la crise diplomatique franco-suisse qui s'en est suivie, a été le révélateur cruel et paradoxal de ce que le secret bancaire a pris, depuis quelques années, une valeur proportionnelle à la vitesse de son déclin.

Jadis, le secret bancaire suisse s'évoquait avant tout en relation avec les seules politiques fiscales étrangères, souvent voraces sinon opportunistes, ou avec quelques comptes criminels – rescapés d'une époque révolue – qui auraient échappés à la vigilance des services compliance, lesquels appliquent avec rigueur la loi fédérale sur le blanchiment d'argent (LBA), l'une des plus rigoureuses au monde, omet-on souvent de rappeler, surtout à l'étranger.

Au cours des dernières années, la relation triangulaire qui prévalait jusqu'alors entre les banques suisses, la justice helvète et les fiscs étrangers, initialement basée sur le respect tant des lois internes que des conventions passées avec nos Etats partenaires, a été foulée au pied aussi bien par les détracteurs de notre finance que par les pays «amis». Exit les conventions, au sens propre comme au figuré; la crise est passée par là et le délit fiscal est devenu raison d'Etat.

Surfant sur la vague de l'affaire UBS aux Etats-Unis, véritable boîte de Pandorre, nos voisins européens ont emboîté le pas aux américains en déléguant à leur administration fiscale et à leurs services de renseignement la traque aux fraudeurs, coupables désignés – et dès lors un peu schématiques – d'une économie européenne déclinante. Une nouvelle doctrine émerge alors sous les traits d'une sorte d'ingérence fiscale indirecte, aux allures de légitime défense internationale, dont le fondement serait l'acceptation de la violation du droit suisse, voire même un encouragement à celle-ci. Si la presse, mi-fascinée mi-incrédule, se plaît à rattacher à demi-mot ces pratiques au roman d'espionnage, il reste qu'Hervé Falciani a été approché, recruté, employé et protégé exactement comme l'aurait été un agent.

Cette affaire, pour emblématique qu'elle soit, n'est évidemment que la partie émergée de l'iceberg, puisque de nombreux autres dossiers similaires, dont l'achat par le land allemand de Rhénanie-du-Nord-Westphalie d'un disque contenant des données elles aussi volées et la mise en œuvre de près de deux-cent perquisitions sur son sol, ont émaillé la tranquillité des rapports avec nos voisins. Au delà des cas particuliers, l'attitude de certains de nos voisins a créé une véritable demande, les données confidentielles devenant ainsi l'objet d'une forme de marché noir transfrontalier dont les échanges s'avèrent aussi occultes que fructueux. En 2018, l'échange automatique d'informations appelé à être instauré devrait certes permettre d'apaiser certaines tensions mais gageons que ce serait faire preuve de trop d'angélisme d'espérer qu'elle entraînera une tabula rasa des mauvaises pratiques du passé et qu'elle préviendra, dans l'intervalle, de nouvelles tentatives de vol de données.

LES DONNÉES CONFIDENTIELLES SONT L'OBJET D'UNE FORME DE MARCHÉ NOIR TRANSFRONTALIER AUX ÉCHANGES AUSSI OCCULTES QUE FRUCTUEUX.

Parallèlement à ces affaires internationales et très médiatisées, la finance helvétique se découvre depuis plusieurs années un nouvel ennemi redoutable, parce que rarement identifié, le pirate informatique. Pas un mois ne se passe sans qu'une banque ou l'un de ses clients ne soit victime d'une tentative de hameçonnage, d'un cheval de Troie ou d'une intrusion informatique, avec pour victimes en première ligne les clients dont les comptes sont frauduleusement siphonés ou qui voient leurs noms dévoilés sans ménagement sur Internet. Viennent ensuite les banques dont l'image est souvent sérieusement écornée.

Davantage que la fréquence des attaques, ce qui frappe dans la criminalité informatique en la matière, c'est le changement de stratégie des pirates. Ainsi, en marge de la piraterie que l'on pourrait qualifier d'économique, et qui vise premièrement l'acquisition illégale de fonds, on constate l'émergence forte d'une piraterie «institutionnelle» qui vise l'obtention en tant que telle d'informations bancaires. Force est de constater que les données bancaires ont désormais une valeur propre correspondant à celle que des Etats ou des individus sont prêts à payer pour les obtenir ou, plus pernicieusement, celle que la banque et ses clients sont prêts à débourser pour les garder secrètes.

En ligne de mire de ces nouveaux pirates de la géopolitique fiscale, on retrouve notamment la Suisse, le Luxembourg et les autres pays figurant sur les listes grises et noires établies par l'Organisation de coopération et de développement économiques (OCDE). A cet égard, l'affaire de la Banque Cantonale Genevoise (BCGE), dont certaines données confidentielles ont été dérobées et que les pirates menaçaient de rendre publiques si une rançon n'était pas versée, est symptomatique de ce nouveau péril.

Ces différents exemples, tant sur le plan des relations fiscales internationales que sur celui du crime organisé, attestent de ce que le secret bancaire a connu au cours de ces dernières années un véritable changement de paradigme, qui dépasse, et de loin, la simple érosion juridique. Chaque information couverte par le secret bancaire a désormais un prix, des acheteurs et des vendeurs.

D'un point de vue interne aux banques, ces nouveaux risques impliquent de repenser entièrement la politique de sécurité, allant de l'engagement des employés (généralisation des background checks) à la ségrégation des données, en passant par la sécurisation forte de ces dernières.

Du point de vue législatif, le Conseil fédéral a été chargé de préparer les modifications légales visant à sanctionner de manière appropriée l'utilisation et la transmission, gratuite ou contre rémunération, de données bancaires acquises illicitement, ce qui contribuera à limiter, ou à tout le moins à dissuader, les velléités d'employés indélicats. Ce n'est qu'au prix de ces efforts que la Suisse parviendra, tant sur le plan extérieur qu'à l'intérieur de ses frontières, à assurer la pérennité de son système bancaire et la confiance qu'il continue à ce jour d'inspirer. ■

**Respectivement avocat aux barreaux de Genève et Paris (liste des avocats communautaires) et titulaire du brevet d'avocat.*