Comment les banques externalisent leurs données sensibles au nez de l'ANSSI

Le siècle de la donnée :

La Loi de Programmation Militaire 2014-2019 (LPM), impose aux organismes désignés « d'importance vitale » (OIV), de renforcer la sécurité de leur système d'information. La liste des OIV est confidentielle, mais laisse peu de doutes sur les opérateurs privés ou publics dont les activités sont vitales pour la France, tels que les transports, la santé, l'énergie, les télécom.. et bien sûr, la finance. Les banques, Banque Centrale incluse, font aussi partie de cette liste. Avec l'avènement de la loi, l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) s'est vue attribuer de nouvelles prérogatives, comme celle d'imposer aux OIV de protéger contre toute *indisponibilité ou destruction par suite d'un acte de malveillance de sabotage ou de terrorisme qui risquerait, directement ou indirectement d'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation*[i]. L'application de cette loi soumet l'opérateur d'importance vitale a de nombreuses contraintes et obligations, à ses frais : détecter et signaler les incidents à l'ANSSI, mettre en œuvre des moyens techniques qualifiés, soumettre son système d'information d'importance vitale (SIIV) à un audit annuel, réalisé par des prestataires agréés.

Dans la même fenêtre temporelle, un phénomène nouveau s'est emparé des entreprises : l'accélération spectaculaire de leur numérisation, à la faveur des avancées technologiques. Associée à une dimension stratégique et humaine, la transformation digitale des entreprises a fait émerger un trésor inestimable, facteur de croissance et objet de convoitise : la donnée ! et dans le domaine bancaire ce n'est pas n'importe laquelle : la donnée bancaire ! Celle qui contient nos petits et grands secrets, celle qui montre nos revenus, qui explique notre façon de consommer, celle qui montre nos abonnements, nos voyages et combien de fois nous allons chez le médecin. Une pépite inestimable, le pétrole du 21e siècle comme on l'appelle désormais. Comme toute opération d'achat et de vente, de tout et de rien, de tous les citoyens, transite forcément par son compte en banque, toute l'information est concentrée au même endroit.

Comparé à celle récupérée par les navigateurs internet qui déduit un comportement, une donnée bancaire permet un vrai profilage ciblé du client. Les banques ne disposent pas seulement des données de leurs clients ; des données tout aussi sensibles mais bien plus stratégiques sont également présentes dans les systèmes d'informations : les données des entreprises clientes en sont un exemple mais également les portefeuilles d'investissement pour compte propre ou pour la clientèle. La Banque Centrale française n'échappe pas à cet instrument de pouvoir : elle exerce en effet une activité de trading comme n'importe quelle banque d'investissement[ii], en plus de sa clientèle institutionnelle, la Banque de France gère des réserves de change sous la forme de portefeuilles obligataires investis sur le marché des devises et procède donc à des opérations d'achats-ventes de devises. On le voit donc, désormais plus aucune donnée bancaire, particulière ou institutionnelle n'a échappé à la digitalisation. La donnée est un vrai instrument de pouvoir.

Ça commence par l'externalisation de fonctions non-sensibles…

Contraintes ou opportunistes, à la faveur des concurrents non-bancaires, de la législation l'accompagnant, et des fortes obligations réglementaires[iii] les banques ont dû innover et s'adapter rapidement aux nouvelles technologies permettant l'exploitation des données.

Poussées par leurs utilisateurs de la génération Y, sommées de réussir leur transition digitale pour permettre la connexion d'acteurs externes[iv], les banques ont investi massivement dans la construction de leur cloud privé.
Malheureusement toutes n'ont pas réussi. Trop cher, pas assez agile, il est souvent délaissé au profit de clous privés[v] : Microsoft, Amazon pour ne citer qu'eux, leur offre de la souplesse, de l'adaptabilité aux besoins métier et des économies substantielles de ressources internes. La Société Générale et la BNP ont ainsi basculé leur messagerie dans Office365, la suite bureautique de Microsoft hébergée dans le cloud[vi], la Société Générale a fait le choix pour son archivage de mails de la société Global Relay, une société canadienne de services de messagerie dont le siège se trouve à Vancouver. Crédit Mutuel a fait le choix d'AWS le cloud d'Amazon pour sa capacité à fournir des services d'intelligence artificielle, grande consommatrice de données. On pourrait penser que la messagerie n'est pas représentative des données personnelles et confidentielles ; pourtant, combien de fois, vous, lecteur, avez transmis une information sensible par mail sans spécialement le chiffrer ? combien de fois avez-vous écrit un document bureautique sans spécialement le classifier ?

Pour ensuite externaliser des masses de données
Malgré les réglementations strictes sur les données bancaires et les données personnelles, malgré les recommandations de l'ANSSI sur l'externalisation des données[vii], on observe, encore beaucoup trop souvent, un autre phénomène d'externalisation, mais cette fois lié à la fonction de surveillance, de conformité, et de supervision. Sous le prétexte d'une mise en conformité aux règlements européens de façon rapide, pratique et à moindres coûts, de grands éditeurs américains ont très vite compris l'importance de produire des suites logicielles hébergées dans leur cloud et proposant des facilités qu'aucune entreprise européenne ne peut leur offrir[viii].
Ainsi Global Relay qui traite les archives mail propose également des outils de surveillance dans le cloud, permettant de garantir la conformité à des réglementations comme MAD2 relative aux abus de marché, la solution est utilisée par certaines banques comme la Société Générale pour ne donner que cet exemple. Thomson Reuters ne s'y est pas trompé. En rachetant la petite société Bnext, elle permet également de traiter la même problématique d'abus de marchés et récupère ainsi les données de comptes titres des clients bancaires. La Banque Privée Société Générale ou Börse Stuttgart[ix] les a choisis[x]. Nasdaq n'échappe pas à la règle, avec sa suite SMARTS, elle permet aux banques Françaises et européennes de vérifier la conformité de leurs opérations de trading. Ce faisant, elle récupère au passage toutes les données de trading de la banque (nom du trader, de la contrepartie, de l'instrument échangé...).
Sur la réglementation relative au blanchiment d'argent et financement du terrorisme, la société SAS, américaine, n'est pas en reste : grâce à l'intelligence artificielle, elle offre des capacités d'analyses de données et de profiling client impressionnantes il a été choisi par le Crédit agricole, le Crédit du Nord et la Société Générale. Sur les marchés financiers, Quod Financial, société anglaise propose aux banques centrales une plateforme d'opérations de change et de gestion des liquidités destinée aux banques, et hébergée hors Europe. Utilisée par la Banque de France[xi], elle permet aux traders de la Banque de participer aux missions régaliennes de politique monétaire et stabilité financière de l'Eurosystème. La liste est longue, et on peut également citer Tradefeedr, société anglaise, qui a développé un outil d'aide à la décision, grâce à un puissant agrégateur de données de trading, dans le cloud. Il est utilisé par BNP et par la Banque de France. Même stratégie chez DTCC, leader mondial

américain du traitement de la donnée post-marché. En rachetant la totalité des parts d'OMGEO[SM] en 2013, elle devient la référence mondiale en matière d'efficacité du traitement post-trade des actifs institutionnels et met la main sur les données de la Banque Centrale Européenne[xii]. La DTCC exploite des installations à New York et dispose de bureaux dans 14 pays.
Tous les éditeurs, à quelques exceptions près (Nasdaq, Bnext…), proposent leurs solutions en version locale, (dans les locaux du client) ou en version « Cloud » mais dans la plupart des cas, il faut envoyer les données dans leur cloud si l'on veut bénéficier de toutes les fonctionnalités. Et lorsque l'Entreprise choisit le mode local, il faut tout de même faire intervenir l'éditeur à distance pour des problématiques de maintenance applicative, et donc lui donner accès au système d'information local.

Et se termine par l'absence totale de discernement :
Comment se fait-il que l'ANSSI, ou ses partenaires qualifiés, censés auditer ces systèmes d'importance vitale (lorsqu'ils sont désignés comme tels), ne constatent pas ces excès d'inconscience, et cette absence de maitrise du risque ? comment se fait-il qu'aucun organisme d'audit indépendant (l'ACPR, l'AMF) ou les services d'audit interne des Banques Centrales, ne tirent la sonnette d'alarme sur la quantité de données bancaires sensibles hébergées désormais dans des clouds privés américains ou anglais? Est-il possible que ces garde-fous qui devraient protéger de ce type d'erreurs et d'absence totale de discernement se soient concentrés sur le contenant (le système) et pas le contenu (la donnée) ? Et qu'il ait suffi à l'organisme d'importance vitale, juste de désigner le SIIV objet de l'audit, sans que l'auditeur ne s'inquiète de la donnée qu'il contenait et de son usage? Il y a de quoi s'interroger.
En 2011, à l'initiative de la France, le projet Andromède, qui visait à doter l'Europe d'un cloud souverain[xiii] s'est très vite scindé en 2 projets en raison d'un désaccord entre les protagonistes. Mais Cloudwatt, porté par Thalès et Orange, financé par l'état à hauteur de 75M€, s'est arrêté en février 2020 et les utilisateurs sommés de retirer leurs données, quant au second projet, Numergy, il a été placé en procédure de sauvegarde dès 2015 et entièrement racheté par SFR, l'un de ses fondateurs, en 2016.
On le voit, le chemin de la prise de conscience est long, il demande une volonté politique afin de combler les manques dans plusieurs domaines : la recherche scientifique et la technologie, car ce n'est pas les datascientists qui manquent en France, ce n'est pas les développeurs, ni les terrains pour construire des centres d'hébergement mais bel et bien une véritable culture du risque et de l'anticipation en entreprise, une vision stratégique sur la donnée, et une dynamique de soutien de l'état aux pépites françaises et européennes à l'instar de ce qui s'est passé tout récemment pour Photonis, sauvée in-extremis d'un rachat américain. Aujourd'hui il manque à l'Europe un fonds souverain pour protéger la base technologique et renforcer ce précieux capital de la donnée.

[i] Article L1332-1 du code de la défense
[ii] https://www.lesechos.fr/finance-marches/marches-financiers/la-banque-de-france-championne-du-trading-134237
[iii] DSP2, MAD2, FATCA, LCB/FT

[iv] DSP2 est la directive qui a instauré l'Open Banking, et qui permet, entre autres, aux acteurs tiers, d'accéder aux données d'un client d'une banque via une API

[v] https://www.lesechos.fr/finance-marches/banque-assurances/les-banques-francaises-au-pied-du-mur-pour-basculer-pour-de-bon-dans-le-cloud-142447

[vi] https://www.avanade.com/fr-fr/media-center/press-releases/societe-generale

[vii] https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

[viii] Ou lorsqu'elles existent, les pépites se font vite racheter par des américains, c'est le cas de Dataïku.

[ix] bourse allemande, la deuxième plus grande du pays et la neuvième en Europe

[x] https://www.b-next.com/about/references/

[xi] https://www.agefi.fr/asset-management/actualites/quotidien/20180605/banque-france-se-dotera-d-agregateur-forex-249102

[xii] https://www.ecb.europa.eu/paym/pdf/cons/t2s/t2s-2_Omgeo.pdf?68a2d30b4a0d5813996750ccc955dab9

[xiii] https://fr.wikipedia.org/wiki/Androm%C3%A8de_(cloud)