Réunion du Groupe des superviseurs bancaires francophones (GSBF)

7 décembre 2020

Discours de clôture de Denis Beau, Premier sous-gouverneur

« Les enjeux de la résilience opérationnelle »

Mesdames et Messieurs, chers collègues,

Je suis très heureux de prendre la parole aujourd'hui pour clôturer les travaux de la réunion plénière du Groupe des superviseurs bancaires francophones, (GSBF) que préside depuis 2019 la Banque centrale du Maroc.

Comme vous le savez, l'ACPR est profondément convaincue de l'intérêt des travaux de ce groupe, qui permet tout à la fois de partager nos expériences et nos pratiques de supervision. Les échanges sont particulièrement utiles et précieux, en particulier dans la période actuelle où l'on observe une intensification chez les banques de risques bien connus des superviseurs, au premier chef le risque de crédit, mais aussi la montée de nouveaux risques.

Pour conclure cette réunion, je souhaitais évoquer avec vous une thématique qui prend une ampleur grandissante en matière de supervision des risques auxquels les établissements bancaires font face, à savoir celle de la résilience opérationnelle. Cette notion désigne la capacité d'une institution financière à assurer la fourniture des opérations critiques dont elle a la charge, y compris en cas de perturbation grave. Toutes les institutions que nous supervisons font régulièrement face à des crises de natures diverses, et nous devons nous assurer qu'elles sont capables d'y résister et de poursuivre leurs activités. La problématique de la résilience opérationnelle présente ceci de particulier qu'un

établissement viable économiquement et solvable est cependant susceptible de disparaitre en cas d'incidents opérationnels graves l'affectant directement ou, par contamination, ses parties prenantes. Le sujet a été identifié dans le cadre bâlois sous l'angle du risque opérationnel dès le début des années 2000 avec la peur du fameux « *bug* de l'an 2000 ». Toutefois, il s'agissait d'une première réponse et les dispositions visant à encadrer ce risque étaient, jusqu'à récemment, de nature essentiellement quantitative. Ce cadre me paraît désormais insuffisant pour guider la gestion d'un risque qui se complexifie dans ses sources et dont l'impact sur les institutions et le système financier plus globalement est susceptible de s'intensifier et s'élargir. Cette complexification des sources et cette intensification des impacts potentiels a de nombreux vecteurs. Je voudrais en souligner simplement trois.

Le premier est l'interconnexion croissante des banques, désormais interdépendantes tant pour des raisons financières qu'opérationnelles : elles utilisent les mêmes infrastructures de marché et de paiement et développent de plus en plus souvent des projets communs. Cette situation est renforcée par la présence de plus en plus marquée de prestataires auprès desquels elles externalisent certaines fonctions, et qui parfois travaillent pour de nombreux autres établissements financiers. C'est par exemple le cas des prestataires de *Cloud*. Le nombre d'acteurs interconnectés est ainsi démultiplié, de même que les possibilités de contamination en cas de difficultés : au-delà des conséquences subies par une banque en particulier, des perturbations peuvent affecter l'ensemble du secteur via différents canaux, et se transformer plus globalement en crise de confiance dans le système financier. Les établissements doivent donc prendre en compte dans leur gestion des risques la dimension systémique de ce sujet.

Le deuxième vecteur que je voudrais souligner, c'est la place croissante, et désormais centrale, prise par les technologies et les systèmes d'information dans le fonctionnement des acteurs du système bancaire ; je pense évidemment aux « FinTechs », mais pas uniquement : l'utilisation systématique des outils

numériques, par l'ensemble des institutions financières, les expose à un risque informatique croissant et peut affaiblir leur résilience opérationnelle, notamment dans un contexte de cyber-attaques de plus en plus sophistiquées. Ces attaques peuvent avoir des conséquences lourdes sur la résilience opérationnelle des banques, surtout lorsque les fonctions essentielles, pour les institutions ou l'économie dans son ensemble, sont ciblées et fragilisées. Il peut s'agir aussi bien d'atteintes à des systèmes strictement internes, par exemple le chiffrement d'une base de données par un rançongiciel (plus connu sous le terme anglais de « *ransomware* »), ou des atteintes à des fonctions externes, comme la paralysie de services bancaires en ligne. Ce fut le cas par exemple très récemment, début septembre, pour l'une des trois grandes banques chiliennes, Banco Estado, dont de nombreux services et plusieurs succursales furent fermés pendant plusieurs jours à la suite d'une attaque informatique. Il s'agit de la dimension technique du problème, mais aussi de sa dimension « humaine » : les cyber-attaques atteignent souvent leur cible en profitant du manque de vigilance des utilisateurs.

Le troisième vecteur, c'est la matérialisation de risques à probabilité faible et de portée globale, comme la pandémie que nous traversons, qui conduisent à une activation par un nombre massif d'acteurs pour de longues périodes de plans de continuité d'activité. Ainsi, la crise actuelle due à la Covid-19 met à l'épreuve les capacités de résilience individuelles et collectives des établissements. En France, et plus largement dans la zone Euro, nous n'avons pas eu à déplorer d'incident majeur lié à cette crise sanitaire. Pour autant, nous devons rester vigilants car cet épisode peut être considéré comme un test « en grandeur réelle » des capacités de résilience opérationnelle des établissements, individuellement et collectivement.

J'ai conscience des différences structurelles entre les écosystèmes bancaires, impliquant que tel ou tel vecteur de risque opérationnel puisse avoir un caractère plus ou moins saillant selon les juridictions, mais il me semble que tous les superviseurs du GSBF font face à ces évolutions.

C’est pourquoi la préservation et l’amélioration de la résilience opérationnelle du secteur bancaire appellent une évolution de la règlementation pour mieux guider les établissements dans la gestion de leurs risques opérationnels, et en particulier sur le plan de leur cyber sécurité.

Depuis quelques années, le sujet de la résilience opérationnelle, et singulièrement sa dimension « cyber », est discuté aux niveaux international et européen afin de conduire l’ensemble du secteur financier à un meilleur niveau de résistance. Au niveau international, le Comité de Bâle a ouvert une consultation publique qui s’est achevée en novembre dernier et qui doit déboucher sur l’adoption de nouveaux principes de résilience opérationnelle. Cette publication s’est accompagnée de la mise à jour des principes de gestion du risque opérationnel, car ces deux notions sont fortement liées. Aussi, il est nécessaire que les institutions articulent correctement leurs fonctions de gestion du risque opérationnel et leurs processus de résilience dans divers domaines tels que la gouvernance, l’appétit au risque ou la gestion du changement.

Au niveau européen, la Commission européenne, dans le cadre du « paquet » sur la finance numérique, a publié en septembre 2020 un projet de règlement relatif à la résilience opérationnelle numérique du secteur financier (intitulé « DORA » – *Digital Operational Resilience Act*). Ce cadre, qui a pour objectif d’améliorer la solidité numérique des acteurs financiers et d’harmoniser les réglementations, repose sur quatre piliers principaux : la gestion du risque informatique, le traitement des incidents de sécurité, les tests de résilience et la gestion du risque de tiers avec notamment – et c’est la principale innovation institutionnelle de ce projet – la proposition d’une surveillance directe par les superviseurs des prestataires les plus importants pour le secteur financier. Ce texte est en cours de discussion, avec un objectif de finalisation en 2021.

Toutes ces évolutions règlementaires sont bienvenues car elles permettront aux institutions financières de mieux identifier les menaces, de se protéger contre les défaillances potentielles et de réagir efficacement si nécessaire. Elles seront

ainsi mieux préparées face aux diverses crises afin de continuer à répondre aux besoin de leurs clients, de leurs partenaires et des autorités.

Ce nouveau cadre améliorera également le travail de supervision de la résilience opérationnelle des établissements. Par la mise en place de nouveaux outils, les superviseurs pourront analyser plus finement le niveau de risque des banques.

Pour conclure, je suis convaincu que face à des crises et des menaces globales, à l'image de la pandémie actuelle ou des cyberattaques à l'échelle internationale, il est primordial que les superviseurs échangent sur leurs meilleures pratiques, partagent leurs expériences et collaborent le plus étroitement possible. Il s'agit là de la vocation première du GSBF, qui constituera donc le cadre naturel pour accueillir vos travaux sur ce sujet.

Je vous remercie de votre attention.