BANQUE DE FRANCE
EUROSYSTÈME

ASSEMBLÉE NATIONALE

MISSION D'INFORMATION SUR LA RESILIENCE NATIONALE

Audition de Denis Beau, Premier sous-gouverneur, Banque de France

Mercredi 27 octobre 2021

Monsieur le Président,

Monsieur le Rapporteur,

Mesdames et Messieurs les députés,

L'évaluation et le développement de la capacité du système financier à résister aux chocs, ce que l'on appelle la résilience, et à ne pas les transmettre à l'économie réelle, sont des préoccupations importantes pour la Banque de France et l'ACPR, du fait du mandat qui leur a été donné de veiller à la stabilité du système financier.

Dans le cadre et à la lumière de ce mandat, je voudrais vous présenter (1) les enseignements que nous tirons de la crise sanitaire pour la résilience financière et opérationnelle du système financier français, (2) les actions que nous menons pour soutenir le développement des dispositifs de prévention et de gestion des crises qui exercent une influence très forte sur la résilience de notre système financier.

1. Le retour d'expérience post Covid-19

Je voudrais d'abord tirer quelques leçons en matière de résilience financière à la crise qui nous a frappés en 2020 :

- Alors qu'en 2008 les banques étaient à l'origine de la crise et un vecteur de diffusion et d'amplification de celle-ci à travers le système financier et l'économie réelle, elles ont en 2020 été un vecteur de résistance du système financier à un choc exogène d'ampleur inédite et de transmission des mesures très fortes prises par les autorités publiques, Gouvernement et Banque Centrale Européenne, pour protéger les ménages et les entreprises et pour relancer l'activité.

- Cette capacité des banques à financer l'économie dans les conditions les plus adverses est le résultat de leur résilience financière accrue. Les réformes du cadre réglementaire qui ont suivi la crise de 2008 ont en effet rendu le système financier plus résistant aux chocs, en poussant notamment à un doublement du niveau des fonds propres des établissements bancaires.

- Pour autant, il est important que cette résilience financière soit entretenue et consolidée. C'est dans cette perspective que le Haut Conseil de Stabilité Financière a émis des recommandations sur les conditions d'octroi des prêts immobiliers, recommandations qui viennent d'être transformées en normes, qui protègent ainsi les ménages d'un endettement excessif, et a, depuis 2018, décidé de limiter les expositions que peuvent prendre les principales banques françaises sur les entreprises caractérisées par un fort endettement. Il est également important que cette consolidation puisse s'appuyer, d'une part concernant les banques, sur la mise en œuvre de l'accord dit de Bâle III de Décembre 2017, et d'autre part concernant les acteurs non bancaires, sur une révision de l'encadrement réglementaire du risque de liquidité dans les fonds monétaires et plus largement dans les fonds ouverts.

- La Covid-19 a aussi mis à l'épreuve, via les nouvelles modalités de travail à distance, les capacités de résilience opérationnelle du secteur financier aux niveaux individuel et collectif, notamment face au risque cyber. Il s'agit de la continuité opérationnelle des fonctions critiques, crédits, opérations de marché ou paiements. Nous n'avons pas eu à déplorer d'incident majeur. Pour autant, il est nécessaire de continuer à améliorer le niveau de résilience opérationnelle des services financiers et de ces nouvelles modalités de travail. Cela passe par deux axes, l'un de prévention, et l'autre de gestion des crises, et je voudrais maintenant dire quelques mots sur les actions que nous menons dans cette perspective.

2. Un dispositif de prévention et de gestion des risques

2.1 Notre contribution à la prévention des crises s'appuie sur plusieurs dispositifs, tant micro que macroprudentiels

- Au niveau microprudentiel, le cadre réglementaire du risque opérationnel a été considérablement renforce ces derniers mois. Il s'agit notamment des exigences sur la gestion du risque informatique et de l'externalisation, pour améliorer la capacité des institutions financières à maintenir leurs activités essentielles en cas d'incident grave.

Des modifications règlementaires ont ainsi été apportées au cadre national cette année, en particulier dans le secteur bancaire avec la mise à jour de l'arrêté du 3 novembre 2014. Afin d'insister sur les problématiques de gouvernance du risque, de sécurisation des systèmes d'information et de continuité d'activité, l'ACPR a en outre publié des notices sectorielles (secteur banque et secteur assurance) au mois de juillet, qui lui permettent de mettre en avant les points de vigilance principaux que les institutions financières qu'elle supervise doivent prendre en compte. [*Ainsi, elle rappelle qu'une bonne gouvernance du risque informatique suppose une forte implication des instances dirigeantes (y compris du conseil d'administration) et une organisation du contrôle interne reposant sur une vraie indépendance des équipes de contrôles par rapport aux équipes opérationnelles. En matière de sécurité du système d'information, elle encourage le recours à des dispositifs de cybersécurité qui désormais doivent être considérés comme une base pour tous et non plus comme une option adressée uniquement aux grandes institutions financières (par exemple, mise à jour régulière des configurations de sécurité, chiffrement des données ou encore segmentation des réseaux). C'est d'autant plus une nécessité dans un contexte de recours massif au télétravail qui se pérennise et qui induit une augmentation de la surface d'exposition des entreprises, souvent sans cybersécurité adaptée.*] Sur un plan plus pratique, l'ACPR disposait déjà d'outils de supervision, comme le recours à des tests d'intrusion dans le cadre des contrôles sur place, et les dernières modifications réglementaires en ont introduit d'autres, comme l'accès à un registre centralisé des contrats d'externalisation des institutions financières.

- Les règles édictées au niveau national sont en cours d'harmonisation au niveau européen pour l'ensemble des entreprises du secteur financier à travers la préparation du futur règlement DORA sur la résilience opérationnelle numérique qui nous paraît important et bienvenu. En particulier, parce que ce cadre obligera les établissements à effectuer régulièrement des tests de sécurité et que les autorités financières disposeront d'un nouveau forum européen leur permettant de surveiller directement les prestataires informatiques les plus critiques, comme les fournisseurs de services de cloud.

- Au niveau macroprudentiel, pour prévenir les crises, la Banque de France a développé un diagnostic sur les vulnérabilités et la résilience du système financier dans son ensemble. Ce diagnostic est publié tous les semestres et constitue une base importante des discussions et décisions du HCSF. La dernière édition, parue en juin dernier, souligne

ainsi la vulnérabilité accrue au risque cyber et la nécessité des actions de prévention en la matière.

- La Banque de France met également en œuvre une approche très concrète de la prévention des crises opérationnelles.

  Elle coordonne ainsi des travaux de place via le Groupe de Place Robustesse (GPR) qu'elle préside et effectue des exercices de simulation de crises systémiques.

  - Le GPR est composé des principaux groupes bancaires et infrastructures de marché de la Place, ainsi que des autorités financières et des services de l'État,
  - Il établit des scénarios de crise en s'appuyant notamment sur les analyses issues d'un Observatoire des menaces (ODM), scenarios qui sont ancrés dans le réel -cyberattaque, catastrophe naturelle, défaillance d'un prestataire critique ou encore pandémie-,
  - il organise régulièrement des exercices de simulation ; les derniers en date portaient sur une cyberattaque et ses conséquences (2019 et 2021), la survenue d'une crue majeure en Ile de France (2016).

2.2 L'entretien et l'amélioration des capacités de gestion des crises appellent néanmoins un renforcement des tests et de la coordination au niveau international

- Le dispositif de gestion de crise pour le système financier bénéficie déjà d'une coordination européenne forte.

- C'est l'Eurosystème qui est en charge des décisions concernant la politique monétaire et d'apport en liquidité, en temps normal comme en tant de crise, et qui fournit et opère les infrastructures critiques dans le domaine des paiements de gros montants (Target 2) ou du règlement livraison de titres (T2S). En tant qu'opérateur, l'Eurosystème veille à la résilience opérationnelle de ces infrastructures et mène régulièrement des tests à cette fin.

- Cette coordination européenne, vaut également pour la supervision des risques opérationnels des plus grosses banques de l'Union Bancaire, et donc les principaux groupes bancaires FR, supervisés par le MSU. Le cadre de supervision est appliqué selon les mêmes principes pour tous, et tous ces établissements ont pour obligation d'informer le MSU à propos des incidents informatiques graves qui les affectent. À

l’avenir, DORA incitera aussi les autorités financières européennes à développer un mécanisme d’échange d’information et de gestion de cyber crise à dimension systémique.

- Toutefois, la très grande interconnexion des différentes places financières au niveau international requiert une approche harmonisée de renforcement de la résilience collective.

À l’initiative de la Banque de France, un exercice cyber impliquant 24 autorités financières et des acteurs privés a été organisé lors de la présidence française du G7 en 2019, pour tester la capacité de coordination et assurer une reprise coordonnée des services financiers. Un nouvel exercice de même ampleur pour lequel nous militons est envisagé en 2024, complété par des exercices plus ciblés en 2020, 2021 et 2022.