N°21 / OCTOBRE NOVEMBRE 2016

LES CARNETS DE L'ÉCONOMIE ET DE L'ENTREPRISE

Notre lettre aux parlementaires

EDITO

DE LA SOUVERAINETÉ DU FINANCEMENT DE L'ÉCONOMIE EUROPÉENNE

Qu'il s'agisse de la négociation de traités internationaux ou de la définition de normes par des entités internationales, des exemples récents invitent à s'interroger sur :

- Le fait que certaines organisations internationales et multilatérales, méconnaissent voire ignorent les caractéristiques spécifiques des marchés européens et nationaux ;
- L'absence de contrôle démocratique sur le fonctionnement de certaines de ces organisations.

Le projet actuel du Comité de Bâle visant à compléter les réformes dites de Bâle III, communément appelé Bâle IV par la profession financière (décrit en détail pages 3 et 4), méconnait clairement les spécificités du système de financement européen de l'économie. Celles-ci sont de deux ordres :

- en premier lieu, le **financement des entreprises européennes est assuré pour environ 75% par des financements bancaires et à hauteur de 25% par les marchés**. Le modèle nord-américain est l'exact symétrique : environ un quart des financements sont bancaires et trois quarts par les marchés ;
- en second lieu, la structure du bilan des banques nord-américaines est très différente de celles de leurs homologues européennes. En effet, les **banques américaines cèdent de manière systématique la quasi-totalité de leurs crédits immobiliers – ce qui signifie que leur bilan est allégé d'autant**. Ces crédits seront ensuite « titrisés », le processus étant rendu possible par la garantie, explicite ou implicite, donnée à la quasi-totalité des crédits immobiliers par des agences gouvernementales (Freddie Mac, Fannie Mae, et Ginnie Mae). Faut-il rappeler que les banques européennes ne bénéficient pas, ni au niveau national, ni au niveau européen d'un dispositif analogue ? Il en résulte que les mesures visant à renforcer la structure du bilan des banques sont beaucoup moins «mordantes» pour les banques nord-américaines qu'elles ne le sont pour les banques européennes.

Les derniers travaux du Comité de Bâle sont particulièrement préoccupants. Les négociations sont entrées dans une phase finale, le dispositif devant être validé par les Gouverneurs des Banques Centrales des principaux pays du monde d'ici la fin de l'année et au plus tard dans les premières semaines de 2017.

Tous les acteurs économiques européens seraient touchés, grandes entreprises comme PME étant pénalisées. De surcroît, certains types de financements spécifiques tels le financement immobilier français ou les financements dits spécialisés (aéronautique, transport maritime, infrastructures,...) seraient également particulièrement concernés.

Le modèle nord-américain de financement de l'économie pourrait être imposé à l'Europe au travers des règles prudentielles aujourd'hui en discussion, alors même que la structure de financement des entreprises européennes est totalement différente et que les conditions ne sont pas réunies pour la mise en œuvre d'un tel modèle (profondeur des marchés, existence de grands fonds de pension, agences gouvernementales de garantie, ...) – à supposer qu'elles soient souhaitées.

Si les négociations devaient aboutir en l'état, l'impact sur les banques européennes et françaises en particulier serait majeur. Le Commissaire européen Valdis Dombrovskis évoquait, au début du mois d'octobre, une augmentation de l'ordre de 25% des actifs pondérés en fonction des risques (RWA) pour les banques européennes.

En raison des spécificités du marché nord-américain rappelées ci-dessus, les **banques américaines seraient quasiment exemptées de tout effort**. Le Ministre de l'Economie et des Finances de la France mettait d'ailleurs récemment en garde contre la « discrimination entre les modèles bancaires » instaurée par des institutions comme le Comité de Bâle.

A court terme, **il est essentiel que soit préservé, particulièrement dans le contexte « post-Brexit », la souveraineté du dispositif de financement de l'économie productive en Europe**, au premier rang duquel figure le système bancaire français, dont les établissements comptent aujourd'hui parmi les plus solides et les plus importants d'Europe.

Mais à moyen terme et quel que soit le résultat du processus en cours, les problèmes posés par les propositions du Comité de Bâle et les menaces qu'elles font peser sur l'économie européenne montrent qu'il est opportun de s'interroger sur la gouvernance de ce régulateur mondial. Il faut rappeler que le Comité de Bâle, qui ne dispose pourtant que d'un pouvoir normatif et non du pouvoir législatif, tend à se placer au-dessus des législateurs européens et nationaux, malgré l'absence de contrôle démocratique sur son fonctionnement et en particulier sur le processus de prise de décisions. Il a ainsi, par exemple, fortement critiqué certaines dispositions des textes législatifs européens transposant les accords de Bâle III, considérant que celles-ci s'écartaient desdits accords.

Le Congrès des Etats-Unis s'est récemment ému des risques posés par l'absence de contrôle démocratique ainsi que par l'opacité des travaux de certaines instances internationales et examine aujourd'hui le projet de « Financial Choice Act »[1]. Ce texte consiste en une gamme très étendue de dispositions allant de la protection du consommateur à la structure des banques. L'une de ces mesures concerne la banque centrale américaine (FED) qui, dans le cadre de négociations internationales, devrait publier largement à l'avance (jusqu'à 90 jours avant les réunions en phase finale de négociation !) ses positions ainsi que les études d'impact. Le Parlement européen a également adopté en avril 2016 une résolution plaidant pour une transparence accrue et pour l'instauration d'un véritable contrôle démocratique[2].

Philippe-Olivier ROUSSEAU
philippe-olivier.rousseau@bnpparibas.com
Affaires publiques France, BNP Paribas

1 -Le texte est disponible sur le site http://financialservices.house.gov/choice/

2-Résolution du Parlement européen du 12 avril 2016 sur le rôle de l'Union dans le cadre des institutions et organes internationaux dans le domaine financier, monétaire et réglementaire.

NUMÉRIQUE

La cybersécurité, nouvelle donne stratégique

Le « cyberespace » est devenu un espace stratégique à part entière et sa sécurité est désormais considérée comme un enjeu majeur. Dès 2013, le « Livre blanc sur la sécurité et la défense nationale » qualifiait d'ailleurs la cyberdéfense de « nouvelle donne stratégique ». Cette dimension stratégique découle de (1) la multiplicité des enjeux liés au cyberespace et à sa sécurité et (2) de la forte hausse des attaques ces dernières années. Dans ce contexte, (3) les banques sont évidemment directement concernées et auront un rôle clé à jouer en matière de cybersécurité.

Des enjeux multiples, à la croisée de l'économique, du sociétal et même du militaire…

En France, cyberterrorisme et cyberdjihadisme sont au cœur des préoccupations des pouvoirs publics et en particulier des ministères de l'Intérieur et de la Défense. Une organisation comme Daech, qui a généré 2,5 milliards de dollars de chiffre d'affaires en 2015 et a prouvé sa maîtrise d'internet comme outil de communication, a la capacité financière d'embaucher des ingénieurs informatiques très qualifiés.

Le sujet est également une priorité des autorités européennes. Le Parlement européen et le Conseil ont adopté en juillet 2016 la directive NIS (directive on security of network and information systems), qui définit les nouveaux standards de cybersécurité en Europe. Cette directive s'intègre dans le programme « Digital Single Market » promu par la Commission européenne.

Conséquence inévitable de la numérisation de nos vies professionnelles et de nos vies privées, le cybercrime s'est généralisé et est devenu protéiforme, concernant à la fois les éléments les plus exposés mais également les informations personnelles ou couvertes par le secret des affaires. Les motivations des cybercriminels, pirates des temps modernes, sont variées et ne se réduisent pas à de simples enjeux financiers : ils incluent l'activisme idéologique ou politique, parfois au service ou à l'initiative d'Etats ou d'organisations de type mafieuses.

Leur but peut être le gain financier aussi bien que le vol d'informations confidentielles ou sous embargo.

Les enjeux les plus importants ne sont pas de nature financière mais économique : ils concernent la propriété intellectuelle industrielle. Selon le cabinet de conseil PwC, la croissance des cyberattaques dans le secteur de la propriété intellectuelle a été de 56% en 2015. Et cette croissance s'élève à 193% pour l'industrie financière – pourtant l'une des mieux protégées.

Incidemment, force est de constater que des méthodes de paiement comme les bitcoins, fondés sur la technologie blockchain, ont permis de rendre les transactions financières illégales tout à la fois sûres et anonymes…

Des attaques en forte hausse et de natures diverses, entre failles technologiques et facteurs humains

De manière également très inquiétante, le cabinet Symantec relève qu'aux Etats-Unis, un demi-milliard de données personnelles ont été volées ou effacées en 2015, et que dans 39% des cas, ces vols ont concerné le domaine de la santé. Au début de 2015, l'assureur médical américain Anthem a subi le vol de 78 millions de dossier médicaux personnels. Encore ne s'agit-il là que de chiffres déclarés par les entreprises – ce qui signifie que les chiffres réels sont beaucoup plus élevés.

Quel que soit leur nature, portée, fréquence et gravité, le nombre de cyberattaques continue d'augmenter de façon spectaculaire. PwC relève dans son rapport annuel sur le cybercrime que le nombre d'incidents de cybersécurité, tous secteurs confondus, a cru de 38% en 2015, ce qui représente le taux de croissance annuel le plus élevé depuis 12 ans.

Parmi les différents types d'attaques, celles visant à rendre un service en ligne indisponible en le submergeant de demandes provenant de plusieurs sources [attaques par déni de service distribué (DDoS)] sont de plus en plus nombreuses, comme le montre l'actualité. Dernier exemple en date, l'attaque géante par déni de service subie le 21 octobre 2016 par l'entreprise américaine Dyn, en charge de la gestion des zones DNS (Domain zone systems : système de noms de domaine). L'attaque a rendu inaccessible pendant de longues heures, aux Etats-Unis et dans certains cas en Europe, de nombreux sites majeurs tels que Paypal, Tweeter ou encore Airbnb.

Il semble que, dans ce cas, la cause du problème réside dans « l'internet des choses » (Internet of Things), c'est-à-dire dans les failles de sécurité dans les objets connectés à Internet.

Parmi les objets connectés très répandus et dont le niveau de sécurité sont les plus faibles figurent les télévisions connectées à internet (« smart TVs »), les voitures (on se souvient que près d'un million et demi de véhicules commercialisés par Chrysler

LES ATTAQUES LES PLUS RÉPANDUES

- l'installation de programmes espions,
- l'installation de programmes pirates,
- les intrusions,
- les détériorations diverses,
- la destruction de sites,
- le vol d'informations,
- les dénis de service sur des sites,
- le rebond à partir de sites informatiques victimes.

CHIFFRES ET TENDANCES, TOUS SECTEURS D'ACTIVITÉ CONFONDUS POUR L'ANNÉE 2016

- Près d'un million de menaces par logiciels malveillants (malware) ont lieu quotidiennement.
- Environ 40 000 sites Web sont piratés tous les jours.
- Plus de 33 000 sites d'hameçonnage (phishing, skimming) ont été détectés en une seule semaine soit une hausse de 35 % par rapport à l'année 2015.

Source : Global Economic Crime Survey 2016 PwC

DÉFINITION DE LA CYBERSÉCURITÉ

L'ANSSI (Agence nationale de la sécurité des systèmes d'information), lorsqu'elle a rendu publique en février 2011 la stratégie de la France en matière de défense et de sécurité des systèmes d'information, a défini la cybersécurité comme étant l'« état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles. »

et Fiat ont fait l'objet d'un rappel, car des hackers étaient parvenus à en prendre le contrôle) et… les dispositifs médicaux « pilotés » par Internet, tels des pompes à insuline.

Le cabinet Gartner estime à 6,4 milliards le nombre d'objets connectés en 2016 : 5,5 millions de nouveaux objets connectés chaque jour ! A l'horizon 2020, le monde devrait compter 20,8 milliards d'objets connectés, qui seront très majoritairement détenus et utilisés par des particuliers…

Une étude du Ponemon Institut montre que 64% des responsables IT et Sécurité des banques internationales déclarent avoir subi au moins un DDoS au cours de l'année 2015. En 2016, 73% des entreprises françaises redoutent de subir une cyber-attaque dans les deux prochaines années. 16% des français ont été victimes d'un piratage au cours des douze derniers mois.

La plupart des analyses sur le piratage informatique se concentrent sur les failles technologiques, les défaillances techniques ainsi que leurs méthodes de dispersion et de prolifération. Il semble pourtant qu'un facteur important et souvent sous-estimé soit absent de ces analyses : l'humain. Autrement dit, la composante humaine et sa subjectivité intrinsèque comme source de vulnérabilité majeure qui devient une mécanique inépuisable pour commettre les escroqueries les plus audacieuses.

En 2015, le forum économique mondial de Davos, qui place la cybersécurité au rang des défis majeurs pour l'économie mondiale, estimait que les menaces et risques émanant du cyberespace devaient être traités par les Etats comme par les industries de manière holistique, autrement dit de manière globale, et non en tentant d'expliquer le phénomène en le divisant en parties. La lutte contre les cybermenaces suppose donc une étroite coopération entre l'industrie du net, les pouvoirs publics et l'ensemble des acteurs privés. Cette coopération se matérialise notamment à travers l'émergence des CERT (Computer Emergency Response Team), ces centres de veille, d'alerte et de réponses aux attaques informatiques (informatique de gestion, informatique industrielle, informatique embarquée ainsi que les objets connectés) destinés essentiellement aux administrations et aux entreprises mais dont les informations sont généralement également accessibles aux particuliers. Grâce à ces structures de coopération, la lutte contre le cybercrime prend en compte l'ensemble des aspects économiques, sociaux, éducatifs, juridiques, techniques et militaires.

Le secteur bancaire, acteur clé de la sécurité numérique

Les banques sont évidemment directement concernées par les enjeux de la cybersécurité. La révolution numérique apporte en particulier une nouvelle concurrence sur le marché des services financiers. De nouveaux acteurs, les Fintech, proposent aujourd'hui leurs services à la clientèle des particuliers (gestion des flux [paiements, virements, …], services gestion financière, prêts) comme à celle des entreprises.

La directive sur les services de paiements (DSP2), publiée en décembre 2015, dispose que ces nouveaux acteurs pourront non seulement accéder aux comptes des clients des banques mais également réaliser des transactions. Cette prolifération de nouveaux opérateurs dans un marché qui ne sera pas régulé est susceptible de créer de nouveaux risques pour la sécurité des consommateurs.

Les banques ont et auront, dans ce contexte, un rôle clé à jouer pour deux raisons :

▸ d'une part parce que l'ensemble des sujets liés à la sécurité (confidentialité des données personnelles, conditions d'usage de ces données, sécurité des dépôts et des transferts, …) est au cœur de la relation de confiance entre les banques et leurs clients ;

▸ d'autre part parce que les banques sont aujourd'hui parmi les plus importants fournisseurs de services en ligne sur le plan mondial.

La future porte d'entrée du cyberespace sera l'identité numérique, confirmée pour chaque consultation ou transaction par une authentification forte. Le règlement européen eIDAS, entré en vigueur au 1er juillet 2016, définit un schéma européen de reconnaissance mutuelle des identités numériques notifiées par les Etats membres. La France devra donc se doter, d'ici à 2018, d'un schéma d'identité numérique. Ce règlement a par ailleurs entièrement refondu le régime des «services de confiance» digitaux, maintenant unifié au niveau européen et aux implications très importantes pour la vie des affaires.

La confiance numérique naîtra d'une étroite collaboration entre les pouvoirs publics - qui définiront les schémas nationaux d'identité numérique et garantiront la neutralité de leur mise en œuvre - et le secteur privé, au premier rang duquel le secteur bancaire, qui assurera les investissements ainsi que le déploiement et l'exploitation des infrastructures nécessaires.

Johan NOLEAU
johan.noleau@bnpparibas.com
Sécurité Groupe, BNP Paribas

RÉGLEMENTATION BANCAIRE

« Bâle IV » ne doit pas pénaliser l'économie européenne

A la suite de la crise financière de 2007, des réformes sans précédent ont été adoptées pour réduire le risque systémique, assurer la stabilité financière, renforcer la solvabilité des banques, protéger le contribuable et améliorer la sécurité et la transparence des marchés financiers.

Le Comité de Bâle en particulier, dans le cadre des accords dits de **Bâle III**, a très significativement renforcé les exigences en capital imposées aux établissements de crédit et créé deux nouveaux ratios de liquidité. Pour se conformer à Bâle III, **les banques françaises ont, depuis 2008, plus que doublé leurs fonds propres** et contracté la taille de leur bilan, en veillant cependant à réduire leurs activités prioritairement hors de leurs marchés domestiques pour préserver leur capacité à servir l'économie et les entreprises françaises et européennes.

Mais le Comité de Bâle poursuit ses travaux et souhaite renforcer davantage les exigences imposées aux banques. Il a présenté en plusieurs étapes depuis le début de l'année une nouvelle vague de réformes, appelée « Bâle IV» par la profession[1], l'objectif fixé par le G20 étant que l'ensemble des dispositions soit finalisé d'ici à la fin de l'année 2016.

Ces nouvelles réformes consistent en une refonte fondamentale du dénominateur du ratio de solvabilité[2] et une remise en cause profonde des modèles d'évaluation des risques. Elles vont obliger les banques françaises et européennes, si elles sont adoptées, à réduire massivement, leurs bilan, ce

qui entrainera des conséquences fortement négatives sur le financement des entreprises européennes.

Une refonte complète des méthodes d'évaluation des risques

«Bâle IV» est constitué d'une série de réformes portant sur le calcul des risques présents au dénominateur du ratio de solvabilité.

La refonte envisagée est complète. Elle touche en effet les méthodes d'évaluation de l'ensemble des risques bancaires « traditionnels », autrement dit les risques de crédit (risque de contrepartie), de marché (actions, obligations, dérivés,...) et opérationnels (erreurs de gestion, sinistres, fraude,...).

Mandaté pour réduire la variabilité des résultats des modèles internes[3], le Comité de Bâle a proposé au début de l'année une réforme globale refondant les méthodes standards et remettant en cause les méthodes internes, en limitant leur usage et en imposant des « output floors », c'est-à-dire des planchers en dessous desquels les RWA ne peuvent pas descendre lorsqu'ils sont calculés via ces modèles internes. Il s'agit donc d'un dispositif hybride par lequel la flexibilité du modèle interne est obérée par la méthode standard.

Une augmentation de la charge en capital pour les risques faibles

La remise en cause des modèles internes pénaliserait en particulier le financement des entreprises européennes présentant un bon profil de risque. En effet les modèles internes assurent une adaptation des charges en capital et des tarifs sur la base d'une évaluation précise des risques réalisés. La réduction de la granularité des méthodes d'évaluation des risques et le caractère conservateur des paramètres imposés aux banques et découlant de la réforme se traduirait par des prix de financement moins flexibles. Il convient en outre de rappeler que dans un environnement de taux bas, la composante « risque de crédit » pèse de manière prépondérante dans l'établissement du prix du crédit.

La réforme conduirait de surcroît à imposer des charges en capital élevées pour des risques faibles, un résultat paradoxal, conséquence d'un présupposé erroné selon lequel les modèles internes ne peuvent pas être bien calibrés pour les portefeuilles à faible risque de défaut.

Une nouvelle vague de « deleveraging » des bilans bancaires

Si les propositions initiales de Bâle ne sont pas substantiellement modifiées dans la phase de calibration finale en cours, les nouvelles règles alourdiront significativement les contraintes pesant déjà sur les bilans bancaires et conduiront inévitablement à une nouvelle vague de « deleveraging », qui affectera cette fois directement le financement des entreprises françaises et européennes, les banques n'ayant plus les marges de manœuvre pour épargner leurs marchés domestiques et n'ayant pas la capacité de lever des fonds dans les conditions actuelles de marché et de valorisation des banques.

Selon les dernières estimations, fondées sur les propositions avancées par le Comité de Bâle au cours de l'été dernier, l'augmentation des RWA pour les banques françaises et allemandes s'établirait dans une fourchette comprise entre 20% et 40%. Et l'impact serait le plus marqué pour les grandes banques, les nouvelles règles introduisant une progressivité liée à la taille.

Compte tenu des conditions de marché, les établissements de crédits devront donc à la fois réduire leurs expositions et répercuter une partie de la hausse des charges en capital sur le prix des financements qu'ils octroient (financement court et long terme, financement export, financements spécialisés,...) ainsi que sur les couvertures de risques pour les entreprises (risques de change, de taux,...).

Le financement de l'économie française, principalement assuré par des groupes bancaires d'importance systémique, serait donc parmi les premiers touchés. Au-delà de la France, toutes les entreprises européennes seraient directement concernées puisque leur financement est assuré à près de 75% par les banques - dont 56% par les grandes banques[4].

Le G20 avait pourtant demandé au Comité de Bâle de poursuivre ses travaux « sans augmentation significative de la charge en capital » pour les banques. Constatant que les propositions de Bâle ne respectaient pas ce mandant, le Conseil Ecofin a adopté à deux reprises, le 12 juillet puis le 11 octobre derniers, des conclusions rappelant le cahier des charges du G20. Si le Comité de Bâle n'est pas en mesure de parvenir à ce résultat dans les délais prévus, c'est-à-dire d'ici à la fin de l'année, **il est indispensable qu'il recule l'échéance et prenne le temps nécessaire pour parvenir à des propositions qui respectent réellement le mandat donné (« no significant capital increase ») et maintienne une approche fondée sur les risques réels présentés par chaque actif**.

Hubert d'ETIGNY
hubert.detigny@bnpparibas.com
Affaires publiques France, BNP Paribas

1- Plutôt que de « Bâle IV », les régulateurs préfèrent parler de « poursuite de Bâle III », une expression réductrice au vu de l'ampleur des réformes envisagées.

2- Pour mémoire, Bâle III portait sur le numérateur du ratio, autrement dit la définition des fonds propres et le niveau minimal du ratio.

3- Voir l'encadré « méthode standard et modèles internes »

4- Source : EBA, rapport sur le ratio de levier – août 2016 : les 14 G-SIBS européennes (Royaume Uni inclus) représentent, en taille d'exposition, environ 56% du total de l'échantillon de 246 banques, représentant lui-même 75% du total des actifs bancaires en Europe.

MÉTHODES STANDARDS ET MODÈLES INTERNES

Il existe deux méthodes d'évaluation des risques et donc de calcul des actifs pondérés par le risque (RWA - Risk-Weighted Assets) :

▸ la première est la « méthode standard » : la même pondération est appliquée à tous les établissements bancaires, quel que soit leur taille ou la diversité de leurs activités - et donc de leur portefeuille d'actifs ;

▸ la seconde est dite « modèle interne » et a été préconisée par les régulateurs pour Bâle II : chaque établissement bancaire établit ses propres modèles de gestion et de mesure des risques sur la base des enseignements tirés de son expérience. Ces modèles internes sont alors soumis à l'autorité de supervision bancaire qui en contrôle la pertinence et peut les amender, voire les rejeter complètement. Ces méthodes sont bien adaptées aux établissements bancaires de grande taille offrant une gamme de services bancaires diversifiés - dans la mesure où ils disposent des capacités techniques et financières pour évaluer plus finement leurs expositions.