

ET SI LA PROCHAINE CRISE FINANCIÈRE VENAIT DE LA TECHNOLOGIE ?

DOMINIQUE CHRISTIAN*

En février 2002, Donald Rumsfeld, à l'époque secrétaire à la Défense des États-Unis, déclara lors d'une réunion avec ses collaborateurs : « Comme nous savons, il y a des connus identifiés ; il y a des choses dont nous savons que nous connaissons. Nous savons aussi qu'il y a des inconnus identifiés ; c'est-à-dire que nous savons qu'il y a des choses que nous ne connaissons pas. Mais il y a aussi des inconnus même pas identifiés, ces choses dont nous ne savons pas que nous ne connaissons pas. »¹

Depuis maintenant plus de cinq ans, régulateurs et professionnels se sont attelés à remédier aux insuffisances et aux faiblesses révélées par la crise de 2007-2008. Des mesures très importantes ont été prises pour renforcer la stabilité du système financier. Mais il faut constater que ces actions ont exclusivement concerné des faiblesses et des insuffisances concernant des sujets déjà identifiés, tels que la solvabilité, la liquidité et la gouvernance des institutions financières, leurs modes de surveillance, l'intégrité et la transparence des marchés, etc. Pour l'essentiel, il s'est agi d'éviter la répétition de difficultés similaires à celles qui avaient été observées.

Peu d'attention semble en revanche avoir été portée à l'identification de facteurs nouveaux susceptibles de déclencher des crises. Or divers événements récents ont montré que le système financier pouvait connaître des difficultés de types tout à fait différents de celles observées en 2007-2008 : la presse a ainsi fait état, au début de 2014, du vol de données personnelles concernant plus de 100 000 clients par un collaborateur d'une institution financière coréenne ; en avril, on a en outre annoncé que, dans certains systèmes d'information, avaient été identifiées des lacunes permettant des intrusions.

De telles vulnérabilités conduisent à s'interroger sur la place actuelle de la technologie dans la sphère financière et sur les risques qu'elle pourrait faire naître

* Économiste.

en matière de stabilité. Et, pour reprendre la formule de Donald Rumsfeld, ces sujets se situent-ils dans la catégorie du connu (*known*), de l'inconnu identifié (*known unknown*) ou de l'inconnu même pas identifié (*unknown unknown*) ?

LA SPHÈRE FINANCIÈRE ACTUELLE : DE LA GESTION DE FLUX FINANCIERS AUX TECHNOLOGIES DE POINTE

La finance est d'abord, naturellement, le lieu où se gèrent les flux de paiements et de règlements, les flux de prêts et d'autres formes de financement ainsi que les flux d'épargne et de tous types de placements. C'est également le lieu où se gèrent une part très importante des encours de crédits et, plus généralement, d'actifs financiers ainsi qu'une part très importante des encours de dettes financières. Toutes ces activités sont aujourd'hui très largement dématérialisées et font donc l'objet de traitements automatisés, s'appuyant sur des moyens technologiques toujours plus sophistiqués.

La finance est en outre le lieu où se gère une part considérable des risques encourus par une économie développée. Pour assurer son rôle de couverture des risques, elle doit recourir à des techniques elles-mêmes de plus en plus évoluées et nécessitant des ressources technologiques très avancées.

Mais aujourd'hui, la finance est probablement aussi l'un des domaines économiques les plus concernés par le phénomène *big data*. Plus que tout autre secteur d'activité, elle repose, non seulement pour sa gestion interne, mais aussi pour l'ensemble des opérations qu'elle propose à sa clientèle, sur la disposition et l'exploitation de données dont la quantité défie l'imagination et dont la qualité doit être constamment maintenue. Pour relever les défis liés au *big data*, elle a ainsi besoin de capacités technologiques toujours plus considérables.

Pour répondre à ses besoins, la finance a depuis longtemps développé elle-même des techniques appropriées, notamment en matière comptable, actuarielle, de statistiques et de mathématiques. Au cours des dernières décennies, elle a également recouru de manière croissante à des moyens développés par des entreprises d'autres secteurs, notamment en ce qui concerne les systèmes d'information. Alors qu'elle représente, dans les pays développés, entre 4 % et 8 % du PIB, elle utilise ainsi, selon certaines estimations, de 20 % à 30 % de l'ensemble des produits et des services informatiques.

La finance dépend par suite de plus en plus des développements et des initiatives des entreprises technologiques de pointe. Il n'est donc pas surprenant que celles-ci s'intéressent elles aussi aux activités financières : tel est, par exemple, le cas dans le domaine de la distribution de crédit, comme en témoigne le développement, au cours des quarante dernières années, de GE Capital aux États-Unis, puis dans le reste du monde ; tel est également le cas, aujourd'hui, dans le domaine

des paiements, auquel s'intéressent désormais un nombre croissant de firmes *high tech*, y compris, selon certaines nouvelles, des spécialistes des réseaux sociaux tels que Facebook.

Les évolutions technologiques se poursuivent et se poursuivront encore durablement. Elles continueront donc longtemps à produire des effets sur la finance. Ceux-ci ne se limiteront pas simplement aux modes de gestion et de commercialisation des instruments et des services. Ils s'étendront progressivement à la conception elle-même des instruments et des services financiers ainsi qu'aux bases mêmes de l'organisation des activités et des métiers financiers.

LA TECHNOLOGIE : UN FACTEUR DE RISQUE KNOWN UNKNOWN OU UNKNOWN UNKNOWN ?

Pour la finance, les technologies nouvelles sont incontestablement des aides indispensables à la maîtrise des risques. Mais ne sont-elles pas également des facteurs de risque ?

Les professionnels de la finance ont déjà pris clairement conscience des risques liés à l'emploi de nouvelles technologies. Même si, le plus souvent, ces risques ne sont pas expressément identifiés sous ce terme, ils n'en appartiennent pas moins à la catégorie des risques opérationnels et font dès lors l'objet d'une cartographie périodiquement mise à jour ainsi que d'une évaluation régulière. Des dispositifs appropriés de maîtrise de ces risques existent ainsi sous la forme, en particulier, de plans de continuité d'activité et de modes spécifiques de surveillance de la sécurité des systèmes d'information. Conformément aux principes déjà prévus par l'accord Bâle II et repris dans l'accord Bâle III, les établissements de crédit ayant leur siège dans un pays respectant ces accords doivent publier des informations détaillées sur leur politique de risque et leurs rapports annuels contiennent par suite des indications toujours plus précises sur la manière dont ils font face aux risques opérationnels, donc aux risques technologiques. Dans la mesure où, au sein de l'Union européenne, les entreprises d'investissement sont également soumises aux exigences de Bâle et où, en application de la directive Solvency II, les entreprises d'assurance devront progressivement appliquer des principes similaires en matière de maîtrise de leurs risques, on peut donc considérer que les risques technologiques devraient être convenablement identifiés et maîtrisés par l'ensemble des institutions financières, au moins au niveau individuel.

D'un point de vue plus global, l'identification et, par suite, l'évaluation des risques technologiques paraissent en revanche moins avancées. Au terme d'une revue, peut-être trop rapide, des documents publiés par le Conseil de stabilité financière (CSF), le Comité de Bâle, l'OICV (Organisation internationale des commissions de valeurs), le Fonds monétaire international (FMI)

ou le Comité européen du risque systémique (CERS), il ne semble pas en effet que, depuis la crise de 2007-2008, des études aient été spécifiquement consacrées à la question des risques de caractère technologique. Si plusieurs de ces instances publient périodiquement des statistiques ou des analyses sur certains types de risques, il faut constater que ces informations concernent presque exclusivement les risques à caractère économique et financier et non ceux de caractère technologique ou, plus largement, opérationnel. Et, alors même que chaque établissement de crédit est tenu, en application des accords de Bâle, de revoir périodiquement la cartographie de ses risques, aucune instance mondiale ou européenne ne semble aujourd'hui établir et publier de cartographie régulièrement mise à jour de l'ensemble des risques, y compris opérationnels, auxquels le système financier est exposé, ni ne fournit simplement de synthèse des informations périodiquement publiées par les professionnels en ce domaine.

Il faut donc constater que même si aujourd'hui les risques technologiques semblent être convenablement maîtrisés au plan individuel, le sujet de la maîtrise globale de ces risques relève plutôt de la catégorie des *unknown unknowns* ou, au mieux, de celle des *known unknowns*.

Certes, il est tout à fait légitime que les instances internationales se soient consacrées par priorité à la maîtrise des principaux risques, essentiellement économiques et financiers, dont la crise avait révélé l'insuffisante surveillance, individuelle et collective. De même, il faut convenir que, jusqu'à présent, les risques technologiques, comme plus généralement l'ensemble des risques opérationnels, ont été convenablement gérés par les professionnels.

Il n'en demeure pas moins que plus de cinq ans après le déclenchement de la crise, le moment devrait maintenant être venu de ne plus chercher seulement à remédier à des insuffisances passées, mais de consacrer des moyens adéquats à détecter d'éventuelles faiblesses à venir.

EXPLORER DES TERRITOIRES PEU OU MAL CONNUS

Jusqu'au début du ^{xx}e siècle, dans toutes les cartes du monde figuraient des contrées désignées sous le nom de « *terrae incognitae* ». L'existence de ces contrées était certes connue, de même parfois que leurs contours. En revanche, leur territoire n'avait pas été reconnu et leur cartographie n'avait pas été dressée. Au cours des cent dernières années, des explorateurs, des marins, des aviateurs ont su identifier toutes les parties du globe terrestre et le terme « *terrae incognitae* » n'a désormais plus qu'un caractère historique.

Ce concept peut néanmoins être encore utile en matière de risques encourus par la sphère financière. Il faut en effet avoir la lucidité de reconnaître qu'en raison notamment des évolutions constantes des pratiques, on ne peut, à un moment donné, identifier tous les types de risques qui pourraient un jour affecter les insti-

tutions et les marchés financiers. On ne peut en revanche contester la nécessité de constamment chercher à anticiper et à prévenir la survenance d'éventuels risques systémiques.

Observant les évolutions de la sphère financière depuis plus de cinquante ans, l'auteur a pu constater que, dans un certain nombre de circonstances, professionnels et autorités avaient su prendre collectivement les dispositions appropriées pour éviter le développement ou la propagation de tels risques. Ainsi, la création du Comité de Bâle, décidée à la suite de la défaillance de la banque allemande Herstatt en 1974, a rendu possibles l'instauration d'un dispositif permanent de coopération des autorités bancaires des principaux pays, l'harmonisation progressive des méthodes de surveillance des banques à caractère international et la mise au point de recommandations mondialement respectées en matière de règles prudentielles.

L'action du Comité de Bâle a incontestablement permis d'éviter bien des crises. On peut, par exemple, constater que si les fluctuations particulièrement amples des cours de change des années 1970 et 1980 ont pu provoquer des difficultés individuelles, par exemple celles de la banque Herstatt, elles n'ont pas en revanche provoqué de crise systémique. La coopération entre les autorités y a peut-être été pour quelque chose. De même, l'adoption, par le Comité de Bâle, notamment après la défaillance du Banco Ambrosiano, des principes de surveillance par les autorités du pays du siège ainsi que de surveillance sur base consolidée a permis d'éviter ou de résoudre simplement de nombreuses difficultés individuelles.

Deux exemples montrent, *a contrario*, les conséquences très graves qui peuvent résulter d'un manque de clairvoyance collective :

- alors que dès le début des années 1980, l'Union européenne avait décidé de soumettre tous les établissements de crédit à des exigences prudentielles de même nature, il a fallu, aux États-Unis, attendre la crise des *savings and loans*, à la fin des années 1980, qui coûta au budget fédéral l'équivalent de plus de 5 % du PIB annuel, pour que les autorités décident d'harmoniser les modes de surveillance de leurs diverses catégories d'établissements bancaires ;

- de même, alors que dans l'Union européenne, le principe de surveillance sur base consolidée et celui d'exigences minimales de fonds propres ont été appliqués non seulement aux établissements de crédit, mais aussi aux entreprises d'investissement et aux compagnies d'assurances, c'est seulement après les difficultés rencontrées en 2008 par des groupes aussi importants que Bear Stearns, Merrill Lynch, Lehman Brothers ou AIG que les États-Unis décidèrent de soumettre l'ensemble des institutions américaines d'importance systémique à des normes et à une surveillance prudentielles appropriées.

Ces exemples, d'action comme d'inaction, devraient être médités en matière de risques technologiques. Même si, aujourd'hui, de tels risques n'ont provoqué ni défaillance individuelle, ni, *a fortiori*, risque systémique, il serait préférable de ne pas attendre que des problèmes surviennent pour engager des réflexions et des initiatives appropriées. La crise de 2007-2008 a en effet bien montré

que l'on ne pouvait s'en tenir à l'adage américain traditionnel : « *Don't fix it if it ain't broke.* »

Une réflexion sur les risques systémiques pouvant résulter des évolutions technologiques est certainement une tâche de grande ampleur. Elle devrait d'abord porter sur les domaines particulièrement concernés par ces évolutions, par exemple les systèmes de paiement et de règlement ou la gestion des données, notamment l'externalisation de leur traitement. Elle devrait associer toutes les parties intéressées, c'est-à-dire non seulement les institutions et les autorités financières, mais aussi les fournisseurs de produits et de services. Elle devrait en outre s'attacher non seulement à déterminer les situations susceptibles de conduire à l'apparition de risques globaux et à analyser leurs conséquences éventuelles, mais aussi et surtout à identifier des solutions appropriées afin d'y remédier. Il est clair en effet que les moyens utilisés en cas de crise financière « classique », c'est-à-dire des apports en fonds propres ou en liquidité, ne seraient pas nécessairement d'un grand secours en cas de survenance de risques à caractère technologique.

Dans ces démarches, il serait évidemment utile de capitaliser sur les initiatives déjà prises dans certains pays. Des exemples en ces domaines sont donnés par les exercices menés périodiquement en France en matière de sécurité des systèmes de paiement et d'échanges interbancaires, sous l'égide de la Banque de France avec l'ensemble de la place.

CONCLUSION

L'ampleur et la rapidité des évolutions technologiques constituent des enjeux majeurs pour le bon fonctionnement et la stabilité des systèmes financiers. Même si, jusqu'à présent, ces enjeux ont été convenablement maîtrisés, il est de l'intérêt commun de s'assurer que les risques technologiques ne sont pas seulement gérés de manière appropriée par chaque institution financière prise individuellement, mais qu'ils le sont également au niveau de l'ensemble du système financier.

Ce sont en fait des territoires nouveaux qui s'ouvrent aux réflexions des professionnels, des autorités, des chercheurs et des observateurs extérieurs. Il faut souhaiter que ces territoires aient été explorés avant que surviennent les difficultés.

NOTE

1. « *As we know, there are known knowns ; there are things that we know that we know. We also know there are known unknowns ; that is to say, we know there are some things we do not know. But there are also unknown unknowns, the ones we don't know we don't know.* »