Association des avocats en droit boursier

Paris, 9 septembre 2026

Cybersécurité : le secteur financier face aux risques de dépendance

Discours de Denis Beau

Premier sous-gouverneur de la Banque de France

et Président désigné de l'ACPR

Le secteur financier est engagé depuis plusieurs années dans une transformation numérique profonde pour préserver et développer sa compétitivité, qu'illustre par exemple le poids des budgets informatiques : pour les banques européennes, une étude de la BCE l'estimait à près de 3 % du produit net bancaire en 2024[i].

Les nouveaux outils numériques permettent en effet aux établissements d'attirer de nouveaux clients, en leur offrant de nouveaux ou de meilleurs services, mais aussi de rationaliser les coûts. Pour autant, la transformation numérique a un revers : **elle augmente la surface d'attaque pour les acteurs malveillants**. Or une attaque réussie peut engendrer des coûts importants, à la fois directs et indirects du fait des effets de réputation. Les établissements, tout en innovant, doivent donc veiller à maintenir un haut niveau de cybersécurité.

Pour tenir en même temps ces deux objectifs, et « rester dans la course » à l'innovation, **la solution la plus évidente est bien souvent de recourir aux *hyperscalers***, qui proposent des infrastructures et des services très performants, en particulier en matière de cloud et d'IA, tout en offrant des garanties de sécurité à l'état de l'art. Ce choix **expose cependant à un nouveau risque : la dépendance technologique.** Celle-ci est potentiellement coûteuse sur le long terme : une étude mandatée par le CIGREF avance le chiffre de 264 milliards d'euros dépensés chaque année par les Européens en logiciels et services cloud américains[ii]. Elle est aussi opérationnellement dangereuse, et il n'est pas anodin que le scénario d'un « ***kill switch »*** sur les services numériques américains, longtemps impensable, soit désormais envisagé par le gouvernement[iii]. **La question est donc de savoir si le secteur financier européen peut se permettre, pour atteindre plus rapidement ses objectifs d'innovation et de sécurité, de s'enfermer dans de nouvelles dépendances**. Il est évident que la situation n'est pas simple, et que les établissements doivent composer avec des arbitrages complexes en matière technologique et opérationnelle. Je voudrais passer ici les principaux d'entre eux en revue (I) avant de discuter des solutions disponibles du côté des établissements comme des autorités publiques (II).

*

I/ **Les risques cyber et de souveraineté sont les deux faces d'une même problématique : la maîtrise des infrastructures numériques critiques**. En donnant « les clés du véhicule » à quelques prestataires incontournables sur lesquelles elles n'ont que peu de levier, les entités financières se mettent dans une situation de vulnérabilité, pour au moins trois raisons.

La concentration des fournisseurs constitue en elle-même un nouveau risque opérationnel : l'an dernier, quatorze heures de panne chez AWS ont suffi à suspendre une bonne partie de l'économie en ligne. Ces risques de concentration peuvent d'ailleurs être directement liés à l'usage de mêmes solutions de cybersécurité : ainsi, pendant l'incident CrowdStrike de

juillet 2024, une mise à jour défectueuse a mis en panne 8,5 millions d'ordinateurs à travers le monde.

Ensuite, la dépendance réduit la capacité de maîtrise du risque opérationnel – dont le risque cyber – par les établissements. À force de confier certaines activités à des tiers, **les établissements peuvent perdre la capacité de les réaliser eux-mêmes et, surtout, d'en apprécier pleinement la qualité**. Cette perte d'expertise rend aussi plus difficile le contrôle effectif des prestataires informatiques. Henri Verdier, ancien directeur interministériel du numérique, décrivait ainsi, lors de son audition devant la Commission d'enquête parlementaire sur les dépendances numériques, la « culture, très répandue parmi les DSI, tant dans le secteur privé que dans le secteur public, qui consiste essentiellement à acheter des solutions plutôt qu'à savoir coder soi-même » ; or, ajoutait-il, « lorsqu'une organisation ne sait plus produire elle-même, elle ne sait plus acheter ».

Enfin, en externalisant certains services critiques, les établissements s'exposent à un phénomène d'**« enfermement »** par les fournisseurs (***vendor lock-in***), qui peuvent se matérialiser très concrètement par des augmentations substantielles de coûts une fois la dépendance créée, ou encore par l'obligation de payer des fonctionnalités superflues (pratique du ***bundling***).

Pour autant, malgré ces risques, éviter les dépendances n'est pas simple, d'autant que celles-ci sont souvent déjà bien installées – pensons par exemple à l'usage des logiciels Microsoft sur les ordinateurs professionnels – dans un contexte de renforcement de la menace cyber, sur fond de tensions géopolitiques. En France, toutefois, le secteur financier a peut-être été plus prudent qu'ailleurs, en conservant généralement la maîtrise de ses systèmes les plus critiques.

Le cas des **modèles d'IA de pointe**, comme *Claude Mythos*, fournit un exemple particulièrement éclairant des difficultés à arbitrer entre les différentes solutions. D'une part, il est de plus en plus clair que ces modèles vont constituer un outil incontournable pour la cybersécurité car, à côté des capacités offensives qu'ils peuvent malheureusement offrir aux attaquants, ils apportent de nouvelles possibilités aux équipes de sécurité, tant pour l'identification de vulnérabilités que pour la génération automatisée de correctifs. Recourir à ces modèles paraît donc de bon sens pour « muscler son jeu » en matière de cybersécurité. **Mais tirer pleinement parti de ces solutions suppose souvent de leur accorder un accès très étendu au système d'information de l'établissement, ce qui crée en retour de nouveaux risques** : risque de compromission, mais aussi risque de transfert du capital informationnel du secteur financier vers quelques grands fournisseurs technologiques extra-européens.

II/ Dès lors, que décider, et comment se prémunir face à ces risques de dépendance ? Sans prétendre traiter ici l'ensemble du sujet, je mentionnerai quelques actions qui peuvent être mises en œuvre par les entités financières, et d'autres qui sont à la main des pouvoirs publics.

Les entités peuvent – et doivent – d'abord mettre en œuvre des mesures d'hygiène cyber « de base » : réduire la surface d'exposition, sécuriser les accès, renforcer les capacités de détection et se doter de capacités minimales de réponses aux incidents. Elles doivent aussi s'adapter à l'accélération du rythme d'exploitation des vulnérabilités, ce qui implique de faire évoluer les procédures, les ressources et les outils afin de **déployer plus rapidement** qu'aujourd'hui les correctifs nécessaires. Ces premières recommandations forment le cœur d'une **communication envoyée par l'ACPR aux fédérations professionnelles en juin dernier**.

Les entités peuvent également renforcer la prise en compte des dépendances dans leur analyse du risque opérationnel en réalisant un **inventaire systématique des dépendances critiques** couvrant l'ensemble de leurs actifs informatiques – postes de travail, réseaux, matériels, logiciels, services cloud, équipements de sécurité etc. Bien que complexe, cet exercice est indispensable pour disposer d'une vision complète de l'exposition au risque. Des indicateurs de référence, tels que l'indice de résilience numérique (IRN), développé par un ensemble d'acteurs publics, d'entreprises et d'experts du numérique, peuvent contribuer à cette évaluation[iv].

L'identification des dépendances doit ensuite permettre aux entités d'élaborer des stratégies de résilience opérationnelle. Sur le cloud par exemple, il peut s'agir de recourir à plusieurs fournisseurs (stratégie « multi-cloud »), de conserver les données et applications critiques sur leurs propres serveurs ou sur un cloud privé (stratégie de « cloud hybride »), ou encore de préparer une éventuelle sortie en assurant la portabilité des données et des applications. **Enfin, le recours à des solutions *open source* constitue également une solution intéressante pour réduire les dépendances**.

Évidemment, les autorités publiques ont elles aussi leur rôle à jouer. S'agissant de la règlementation, les enjeux de souveraineté sont déjà bien identifiés au niveau européen : la Commission Européenne a récemment proposé un **« paquet de souveraineté technologique »** intégrant notamment le *Cloud & AI Development Act* (CADA)[v]**.** Ce texte vise à faciliter le déploiement du cloud et de l'IA dans l'UE ; il propose en particulier une classification unique pour évaluer le niveau de souveraineté d'un service cloud[vi]. Le paquet comprend aussi une Stratégie *open source* visant à **assurer un accès continu aux briques logicielles les plus critiques**.

Les autorités de supervision peuvent quant à elles jouer au moins deux rôles complémentaires. En premier lieu, **un rôle de vigie** au travers de leur mission de surveillance.

En soumettant les prestataires informatiques critiques (*Critical Third-Party Providers* ou CTPPs) à un cadre de surveillance commun, DORA permet aux superviseurs financiers de mieux évaluer les risques de concentration, de dépendance et de verrouillage technologique, et donc de mieux articuler les objectifs de sécurité opérationnelle et de souveraineté numérique. En second lieu, les superviseurs peuvent jouer un **rôle de catalyseur** en orientant les pratiques du secteur financier. Cette fonction peut s'exercer à travers la mise en lumière de risques émergents, comme l'a récemment fait le Mécanisme de supervision unique (MSU) en alertant les grandes banques européennes sur les risques liés à l'IA de pointe. Elle peut également passer par **l'exemplarité des choix technologiques** opérés par les superviseurs pour leurs besoins propres, ces choix étant susceptibles d'influencer les décisions des établissements financiers. Enfin, les superviseurs peuvent **soutenir un cadre propice aux initiatives de Place permettant aux entités financières de peser davantage** face aux grands fournisseurs technologiques, comme le *Collaborative Cloud Audit Group* (CCAG) mis en place par plusieurs grandes entités financières allemandes pour réaliser des audits mutualisés des principaux fournisseurs de services cloud.

*

Il existe donc un équilibre, certes délicat à trouver, entre innovation, cybersécurité et souveraineté. Gardons à l'esprit que, malgré l'accélération technologique indéniablement à l'œuvre, **notre résilience collective dépendra de notre capacité à conserver la maîtrise de nos infrastructures ainsi que de nos risques opérationnels**. Intégrer dès aujourd'hui ces enjeux dans nos stratégies est donc indispensable pour limiter les dépendances avant qu'elles ne s'installent durablement. Je vous remercie de votre attention.

[i] BCE, Digitalisation: key assessment criteria and collection of sound practices

[ii] Étude CIGREF, 2025. Chiffres extrapolés à partir des dépenses de 6 grandes entreprises « témoin ».

[iii] Rapport de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France ; voir notamment le chapitre 5 (B)(2)(a).

[iv] aDRI - Indice de Résilience Numérique

[v] Communication sur la souveraineté technologique européenne, accompagnée d'une stratégie de l'UE en matière d'open source | Bâtir l'avenir numérique de l'Europe

[vi] Règlement sur le développement de l'informatique en nuage et de l'IA | Bâtir l'avenir numérique de l'Europe